NENA i3 Standard for Next Generation 9-1-1

Abstract: This Standard provides the detailed functional and interface specifications for a post-transition IP (Internet Protocol)-based multimedia telecommunications system, including the Core Services and legacy gateways necessary to support delivery of emergency calls via an IP-based Emergency Services IP network.

NENA i3 Standard for Next Generation 9-1-1

NENA-STA-010.3b-2021
DSC Approval: 05/18/2021
PRC Approval: 07/09/2021
NENA Executive Board Approval: 07/12/2021
ANSI Board of Standards Approval: 10/07/2021
Next Scheduled Review Date: 07/12/2024

Prepared by:
National Emergency Number Association (NENA) 911 Core Services Committee, i3 Architecture Working Group

Published by NENA
Printed in USA

© Copyright 2011-2022 National Emergency Number Association, Inc.

1 Executive Overview

"i3" refers to the NG9-1-1 system architecture defined by NENA, which standardizes the structure and design of Functional Elements making up the set of software services, databases, network elements and interfaces needed to process multi-media emergency calls and data for NG9-1-1.

This specification builds upon prior NENA publications including i3 requirements [2] and architecture [70] documents. Familiarity with the concepts, terminology, and functional elements described in these documents is a prerequisite. While the requirements and architecture documents describe high-level concepts, the present document describes the detailed functional elements and interfaces to those functional elements. If there are discrepancies between the requirements or architecture documents and this document, this document takes precedence. This document provides a baseline to other NG9-1-1 related specifications.

The i3 solution supports end-to-end IP connectivity; gateways are used to accommodate legacy wireline and wireless originating networks that are non-IP as well as legacy Public Safety Answering Points (PSAPs) that interconnect to the i3 solution architecture. NENA i3 introduces the concept of an Emergency Services IP network (ESInet), which is designed as an IP-based inter-network (network of networks) that can be shared by all public safety agencies that may be involved in any emergency and a set of core services that process 9-1-1 calls[1] on that network (NGCS – NG9-1-1 Core Services). The i3 PSAP is capable of receiving IP-based signaling and media for delivery of emergency calls conformant to the i3 Standard.

Getting to the i3 solution from the current E9-1-1 infrastructure implies a transition from existing legacy originating network and 9-1-1 PSAP interconnections to next generation interconnections. This document describes how NG9-1-1 works after transition, including ongoing interworking requirements for IP-based and Time Division Multiplexed (TDM)-based PSAPs and originating networks[2]. It does not provide solutions for how legacy PSAPs, originating networks, Selective Routers (SRs), and Automatic Location Identification (ALI) systems evolve. Rather, it describes the end state when transition is complete. At that point, SRs and existing ALI systems are decommissioned and all 9-1-1 calls are routed using the Emergency Call Routing Function (ECRF) and arrive at the ESInet/NGCS via

[1] As defined in **Document Terminology**, the term "call" includes text messages and non-interactive calls.

[2] "Originating networks" include service providers who send calls to ESInets/NGCS.

© Copyright 2011-2022 National Emergency Number Association, Inc.

Session Initiation Protocol (SIP). NENA has produced documents covering transition options and procedures.

TDM-based PSAPs are connected to the ESInet/NGCS via a gateway (the Legacy PSAP Gateway). The definition of the Legacy PSAP Gateway is broad enough so this type of gateway may serve both primary and secondary PSAPs that have not been upgraded.

Similarly, the scope includes gateways for legacy wireline and wireless originating networks (the Legacy Network Gateway) used by originating networks that cannot yet create call signaling matching the interfaces described in this document for the ESInet/NGCS. It is not envisioned that legacy originating networks will evolve to IP interconnect in all cases, and thus Legacy Network Gateways will be needed for the foreseeable future. This document considers all wireline, wireless, and other types of networks with IP interfaces, including IP Multimedia Subsystems (IMS) [49] networks, although the document only describes the external interfaces to the ESInet/NGCS, which a conforming network must support. This document describes a common interface to the ESInet/NGCS, to be used by all types of originating networks or devices. How originating networks, or devices within them, conform is not visible to the ESInet/NGCS and is out of scope. The interface conforms to the best practice described in IETF RFC 6881 [46]. ATIS 0700015 [151], which in turn is based on 3GPP TS 24.229 [226] and TS 23.167 [49], describes how IMS originating networks deliver calls to the ESInet/NGCS as defined in this document.

This specification defines a number of Functional Elements (FEs) with their external interfaces. An implementation of one or more FEs in a single indivisible unit (such as a physical box, or software load for a server) is compliant with this specification if it implements the functions as defined, and the external interfaces as defined for the assembly of FEs. Internal interfaces between FEs that are not exposed outside the implementation are not required to meet the standards herein, although it is recommended that they do.

This document describes the "end state" that has been reached after a migration from legacy TDM circuit-switched telephony, and the legacy E9-1-1 system built to support it, to an all IP-based communication system with a corresponding IP-based Emergency Services IP network. To get to this "end state" it is critical to understand the following underlying assumptions:

1. All calls entering the ESInet are SIP-based. Gateways, if needed, are outside of, or on the edge of, the ESInet. Calls that are IP-based, but use a protocol other than SIP or are not fully i3-compliant, must be interworked to i3-compliant SIP prior to being presented to the ESInet.
2. Access Network Providers (e.g., cable providers, DSL providers, fiber network providers, WiMax providers, Long Term Evolution (LTE) wireless carriers, etc.) have

© Copyright 2011-2022 National Emergency Number Association, Inc.

installed, provisioned, and operated some kind of Location Determination and dissemination function for their networks.

3. All emergency calls entering the ESInet/NGCS will normally have location information (which might be coarse, e.g., cell site/sector location in civic or geo-coordinate format) in the signaling with the call.
4. 9-1-1 Authorities have transitioned from the tabular Master Street Address Guide (MSAG) and Emergency Service Numbers (ESNs) to a Geographic Information System (GIS) based Location Validation Function (LVF) and Emergency Call Routing Function (ECRF).
5. 9-1-1 authorities have sufficiently accurate and complete GIS data, which are used to provision the LVF and ECRF. A change to the 9-1-1 Authority's GIS system automatically propagates to the ECRF and LVF and affects routing.
6. All civic locations will be validated by the access network against the LVF prior to an emergency call being placed. This is analogous to MSAG validation.
7. Periodic revalidation of civic location against the LVF will be performed to assure that location remains valid as changes in the GIS system that affect existing civic locations are made.
8. Since the legacy circuit-switched TDM network will very likely continue to be used for the foreseeable future (both wireline and wireless), the i3 architecture defines a Legacy Network Gateway (LNG) to interface between the legacy network and the ESInet/NGCS.
9. Transition to i3 is complete when the existing SR and ALI are no longer used within a jurisdiction. Even after that time, some PSAPs may not have upgraded to i3. The i3 architecture defines a Legacy PSAP Gateway (LPG) to interface between the ESInet/NGCS and a legacy PSAP. The LPG supports the delivery of an emergency call through the ESInet/NGCS to a legacy PSAP as well as the transfer of an emergency call between i3-PSAPs and legacy PSAPs.
10. Federal, State/Provincial, and local laws, regulations, and rules (such as, for example, those specifically referring to ALI and Selective Routers) may need to be modified to support NG9-1-1 system deployment.
11. While NG9-1-1 is based on protocols that are international and are designed to allow visitors and equipment not of North American origin to work with NG9-1-1, the specific protocol mechanisms, especially interworking of legacy telecom and ESInet/NGCS protocols are North American-specific and may not be applicable in other areas.

© Copyright 2011-2022 National Emergency Number Association, Inc.

Table of Contents

1 EXECUTIVE OVERVIEW 2
DOCUMENT TERMINOLOGY 19
INTELLECTUAL PROPERTY RIGHTS (IPR) POLICY 20
REASON FOR ISSUE/REISSUE 21
2 GENERAL CONCEPTS 22
2.1 IDENTIFIERS 22
2.1.1 Agency Identifier 22
2.1.2 Agent Identifier 23
2.1.3 Element Identifier 23
2.1.4 URN Emergency Namespace 23
2.1.5 Services 23
2.1.6 Call Identifier 24
2.1.7 Incident Tracking Identifier 24
2.1.8 LogEvent Identifier 25
2.1.9 Queue Identifier 25
2.1.10 Secure Telephone Identity 25
2.2 TIME 25
2.3 TIMESTAMP 26
2.4 EVENTS COMMON TO MULTIPLE FUNCTIONAL ELEMENTS 26
2.4.1 Element State 26
2.4.2 Service State 28
2.5 LOCATION REPRESENTATION 30
2.6 XCARD/JCARD 31
2.7 EMERGENCY SERVICES IP NETWORKS 31
2.8 SERVICE INTERFACES 33
2.8.1 HTTP Transport 34
2.8.2 Status Codes 34
2.8.3 Versions 34
2.9 REDUNDANCY 36
2.10 TELEPHONE NUMBERS 37
2.11 FUNCTIONAL ELEMENTS 37

© Copyright 2011-2022 National Emergency Number Association, Inc.

3 INTERFACES 37
3.1 SIP CALL 37
3.1.1 Minimal Methods needed to handle a call 39
3.1.2 Methods allowed to be initiated by any UA which MUST be supported by i3 elements 42
3.1.3 Methods used within the ESInet/NGCS 44
3.1.4 Response Codes 45
3.1.5 Header fields and Request URI supported at the interface to the NGCS 47
3.1.6 Header fields Accepted and also used internally 49
3.1.7 Resource Prioritization 51
3.1.8 History-Info and Reason Parameter 52
3.1.9 Media 52
3.1.10 Instant Messaging 56
3.1.11 Non-interactive calls 56
3.1.12 Bodies in messages 57
3.1.13 Transport 57
3.1.14 Call Routing 58
3.1.15 Originating Network Interface 59
3.1.16 PSAP Interface 60
3.1.17 Element Overload 60
3.1.18 Maintaining Connections and NAT Traversal 60
3.1.19 Advanced Automatic Crash Notification Calls 60
3.2 LOCATION 62
3.3 POLICY (POLICIES) 65
3.3.1 Policy Store Web Service 66
3.3.2 Policy Store Replication 74
3.3.3 Route Policy Syntax 75
3.4 LOST 107
3.4.1 Emergency Call Routing using LoST 108
3.4.2 Location Validation 109
3.4.3 <findService> Request 109
3.4.4 <findService> Response 110
3.4.5 locationInvalidated 113

© Copyright 2011-2022 National Emergency Number Association, Inc.

3.4.6 getServiceBoundary 113
3.4.7 listServices and listServicesByLocation 113
3.4.8 Error Responses 113
3.4.9 Warnings 115
3.4.10 LoST Extensions 115
3.4.11 LoSt Query Examples 118
3.5 EVENT NOTIFICATION 120
3.6 SPATIAL INTERFACE FOR LAYER REPLICATION 120
3.7 DISCREPANCY REPORTING 121
3.7.1 Discrepancy Report 123
3.7.2 Discrepancy Resolution 125
3.7.3 Status Update 126
3.7.4 Policy Store Discrepancy Report 127
3.7.5 LoST Discrepancy Report 129
3.7.6 BCF Discrepancy Report 130
3.7.7 Logging Service Discrepancy Report 132
3.7.8 PSAP Call Taker Discrepancy Report 133
3.7.9 SIP Discrepancy Report 133
3.7.10 Permissions/Security/Authentication Discrepancy Report 135
3.7.11 GIS Discrepancy Report 136
3.7.12 LIS Discrepancy Report 138
3.7.13 Policy Discrepancy Report 139
3.7.14 Originating Service Provider Discrepancy Report 140
3.7.15 Call Transfer Failure Discrepancy Report 142
3.7.16 MSAG Conversion Service (MCS) Discrepancy Report 143
3.7.17 ESRP Discrepancy Report 144
3.7.18 ADR/IS-ADR Discrepancy Report 145
3.7.19 Network Discrepancy Report 146
3.7.20 Interactive Media Response (IMR) Discrepancy Report 147
3.7.21 Test Call Generator Discrepancy Report 148
3.7.22 Log Signature/Certificate Discrepancy Report 149
4 FUNCTIONS 151

© Copyright 2011-2022 National Emergency Number Association, Inc.

4.1 BORDER CONTROL FUNCTION (BCF) 151
4.1.1 Functional Description 151
4.1.2 Interface Description 154
4.1.3 Roles and Responsibilities 156
4.1.4 Operational Considerations 156
4.2 EMERGENCY SERVICE ROUTING PROXY (ESRP) 157
4.2.1 Functional Description 157
4.2.2 Interface Description 170
4.2.3 Policy Elements 176
4.2.4 Provisioning 177
4.2.5 Roles and Responsibilities 177
4.2.6 Operational Considerations 177
4.3 EMERGENCY CALL ROUTING FUNCTION (ECRF) AND LOCATION VALIDATION FUNCTION (LVF) 179
4.3.1 Functional Description 180
4.3.2 Interface Description 181
4.3.3 Data Structures 184
4.3.4 Coalescing Data and Gap/Overlap Processing 187
4.3.5 Replicas 189
4.3.6 Provisioning 190
4.3.7 Roles and Responsibilities 190
4.3.8 Operational Considerations 191
4.3.9 Internal and External ECRF/LVFs 193
4.3.10 Relationship Between ECRF and LVF 193
4.4 MSAG CONVERSION SERVICE (MCS) 193
4.4.1 PIDF-LO to MSAG Conversion 194
4.4.2 MSAG to PIDF-LO Conversion 195
4.5 GEOCODE SERVICE (GCS) 196
4.5.1 GeocodeRequest 196
4.5.2 ReverseGeocodeRequest 197
4.6 PSAP 198
4.6.1 SIP Call interface 198
4.6.2 Media 199

© Copyright 2011-2022 National Emergency Number Association, Inc.

4.6.3 LoST interface 199
4.6.4 LIS Interfaces 200
4.6.5 Bridge Interface 201
4.6.6 ElementState 201
4.6.7 ServiceState 201
4.6.8 AbandonedCall Event 201
4.6.9 DequeueRegistration 201
4.6.10 QueueState 201
4.6.11 SI 202
4.6.12 Logging Service 202
4.6.13 Security Posture 202
4.6.14 Policy 202
4.6.15 Additional Data Dereference 202
4.6.16 Time Interface 203
4.6.17 Test Call 203
4.6.18 Testing of Policy Rules 204
4.6.19 Call Diversion 205
4.6.20 Incidents 206
4.7 BRIDGING AND TRANSFERS 206
4.7.1 Attended Transfers 206
4.7.2 Blind Transfers 234
4.7.3 Premature abandonment of a transfer by the Primary PSAP 234
4.7.4 Passing Data to Agencies via Bridging 235
4.7.5 Interoperability Between Transfer Models 236
4.7.6 Conference Bridging for MSRP Text 236
4.8 MEDIA MIXING 238
4.8.1 Mixing of Real-time Text 238
4.9 INTER-ESINET TRANSFERS 239
4.9.1 Upstream Ad Hoc Method to Downstream Ad Hoc Method 240
4.9.2 Upstream Route All Calls Via a Conference Aware UA Method to Downstream Ad Hoc Method240
4.9.3 Upstream Ad Hoc Method to Downstream Route All Calls Via a Conference-aware UA Method241

© Copyright 2011-2022 National Emergency Number Association, Inc.

4.9.4 Upstream Route All Calls Via a Conference Aware UA Method to Downstream Route All Calls Via a Conference Aware UA Method 245
4.10 LOCATION INFORMATION SERVER (LIS) 251
4.11 ADDITIONAL DATA REPOSITORY (ADR) 253
4.11.1 Identity Searchable Additional Data Repository (IS-ADR) 255
4.12 LOGGING SERVICE 256
4.12.1 Logging Introduction 257
4.12.2 Media Recording Interface 257
4.12.3 Log Recording 268
4.12.4 Roles and Responsibilities 289
4.12.5 Operational Considerations 289
4.13 FOREST GUIDE 290
4.13.1 Functional Description 290
4.13.2 Interface Description 291
4.13.3 Data Structures 291
4.13.4 Roles and Responsibilities 291
4.13.5 Operational Considerations 292
4.13.6 Security Considerations 292
4.14 DNS 292
4.15 SERVICE/AGENCY LOCATOR 293
4.15.1 Service/Agency Locator Record Store 294
4.15.2 Service/Agency Locator Search by Location 294
4.15.3 Service/Agency Locator Search by Name 295
4.15.4 Service/Agency Locator Record 296
4.15.5 Service/Agency Locator Inter-ESInet Index 297
4.16 POLICY STORE 299
4.16.1 Functional Description 299
4.16.2 Interface Description 299
4.16.3 Roles and Responsibilities 299
4.17 TIME SERVER 299
4.18 ORIGINATING NETWORKS AND DEVICES 300
4.18.1 SIP Call Interface 300

© Copyright 2011-2022 National Emergency Number Association, Inc.

4.18.2 Location by Reference 300
4.18.3 Additional Data Repository 300
4.19 MAPPING DATA SERVICE (MDS) 300
4.20 OUTBOUND CALL INTERFACE FUNCTION (OCIF) 302
4.21 SECURE TELEPHONE IDENTITY (STI) 305
4.21.1 STI Verification for Emergency 9-1-1 Calls 308
4.21.2 STI Authentication for PSAP-Originated Calls. 309
4.21.3 Call Validation Treatment 309
4.21.4 STI Secure Key Store 310
4.22 INCIDENT DATA EXCHANGE (IDX) 310
5 SECURITY 310
5.1 IDENTITY 310
5.2 PSAP CREDENTIALING AGENCY 311
5.3 ROLES 311
5.4 AUTHENTICATION 314
5.5 TRUSTING ASSERTING AND RELYING PARTIES 315
5.6 AUTHORIZATION AND DATA RIGHTS MANAGEMENT 316
5.7 INTEGRITY PROTECTION 317
5.8 PRIVACY 317
5.9 ALGORITHM UPGRADES 317
5.10 JSON WEB SIGNATURES 318
6 GATEWAYS 319
6.1 LEGACY NETWORK GATEWAY (LNG) 320
6.1.1 Protocol Interwork Function (PIF) 322
6.1.2 NG9-1-1-specific Interwork Function (NIF) 331
6.1.3 Location Interwork Function (LIF) 342
6.2 LEGACY PSAP GATEWAY (LPG) 359
6.2.1 Protocol Interwork Function (PIF) 361
6.2.2 NG9-1-1-Specific Interwork Function (NIF) 372
6.2.3 Location Interwork Function (LIF) 392
6.2.4 Timing at the Legacy PSAP Gateway 393
6.2.5 Trouble Detection/Reporting at the Legacy PSAP Gateway 395

© Copyright 2011-2022 National Emergency Number Association, Inc.

7 DATA AND THE EMERGENCY INCIDENT DATA OBJECT 395
7.1 ADDITIONAL DATA 395
7.2 ADDITIONAL DATA ASSOCIATED WITH A PSAP, THE EMERGENCY INCIDENT DATA OBJECT 397
8 3RD PARTY ORIGINATION 397
8.1 3RD PARTY CLIENT IS REFERRED TO PSAP; PSAP ESTABLISHES CONFERENCE 397
8.2 3RD PARTY CALL AGENT AND CALLER ADDED TO CONFERENCE 400
9 TEST CALLS 402
10 IANA ACTIONS 403
10.1 "URN:EMERGENCY" NAMESPACE 403
10.2 "URN:EMERGENCY:SERVICE" URN SUBREGISTRY 403
10.3 "URN:EMERGENCY:SERVICE:SOS" REGISTRY 403
10.4 "URN:EMERGENCY:SERVICE:TEST" REGISTRY 404
10.5 "URN:EMERGENCY:SERVICE:RESPONDER" REGISTRY 404
10.6 "URN:EMERGENCY:SERVICE:RESPONDER.POLICE" REGISTRY 405
10.7 "POLICE.FEDERAL" REGISTRY 405
10.8 "URN:EMERGENCY:SERVICE:RESPONDER.FIRE" REGISTRY 406
10.9 "URN:EMERGENCY:SERVICE:RESPONDER.EMS" REGISTRY 406
10.10 "URN:EMERGENCY:UID" REGISTRY 406
10.11 "SERVICENAMES" REGISTRY 406
10.12 "SERVICESTATE" REGISTRY 407
10.13 "ELEMENTSTATE" REGISTRY 408
10.14 "URN:EMERGENCY:SERVICE:SERVICEAGENCYLOCATOR" REGISTRY 408
10.15 "SIPHEADERISOPERATORCONDITIONS" REGISTRY 409
10.16 "URN:EMERGENCY:MEDIA-FEATURE" REGISTRY 409
10.17 "QUEUESTATE" REGISTRY 410
10.18 "SECURITYPOSTURE" REGISTRY 410
10.19 "ESRP NOTIFY EVENT CODE" REGISTRY 411
10.20 "ROUTE CAUSE" REGISTRY 411
10.21 "LOGEVENT" REGISTRY 412
10.22 "LOGEVENT PROTOCOL" REGISTRY 415
10.23 "LOGEVENT CALLTYPES" REGISTRY 416
10.24 "CALL STATES" REGISTRY 416

© Copyright 2011-2022 National Emergency Number Association, Inc.

10.25 "LogEvent Announcement Types" Registry 417
10.26 "Non-RTP Media Types" Registry 418
10.27 "Agency Roles" Registry 418
10.28 "Agent Roles" Registry 419
10.29 "Status Codes" Registry 421
10.30 "Interface Names" Registry 422
10.31 "Match Type" Registry 423
10.32 "GIS Layers" Registry 424
10.33 "Policy Type" Registry 425
10.34 "Discrepancy Report Status Token" Registry 427
10.35 "Event Package" Registry 434
10.36 "Agent States" Registry 435
11 IMPACTS, CONSIDERATIONS, ABBREVIATIONS, TERMS, AND DEFINITIONS 435
11.1 Operations Impacts Summary 435
11.2 Technical Impacts Summary 435
11.3 Security Impacts Summary 436
11.4 Recommendation for Additional Development Work 437
11.5 Anticipated Timeline 439
11.6 Cost Factors 439
11.7 Cost Recovery Considerations 440
11.8 Additional Impacts (non-cost related) 440
11.9 Abbreviations, Terms, and Definitions 441
12 REFERENCES 469
APPENDIX A - MAPPING BETWEEN NG9-1-1 AND LEGACY ALI DATA STRUCTURES (INFORMATIVE) 485
APPENDIX B – SI PROVISIONING DATA MODEL (NORMATIVE) 497
B.1 CENTERLINES 498
B.2 STREET/ADDRESS STRUCTURES 502
B.2.1 COMPLETESTREETNAME 502
B.2.2 COMPLETEADDRESSNUMBER 503
B.2.3 STREETSEGMENT 503
B.2.4 COMPLETEADDRESS 504

© Copyright 2011-2022 National Emergency Number Association, Inc.

B.3 SITE/STRUCTURE 505
B.4 STATE BOUNDARY 508
B.5 COUNTY BOUNDARY 509
B.6 INCORPORATED MUNICIPALITY BOUNDARY 509
B.7 UNINCORPORATED COMMUNITY BOUNDARY 510
B.8 NEIGHBORHOOD COMMUNITY BOUNDARY 512
B.9 SERVICE BOUNDARY 513
B.9.1 SERVICE RESPONSE 514
B.10 MSAG 515
B.10.1 MSAG STREET NUMBER EXCEPTION 516
APPENDIX C – SUPPORT FOR PSAP CALL CONTROL FEATURES (NORMATIVE) 517
C.1 ASSUMPTIONS REGARDING BEHAVIOR IN THE ORIGINATING NETWORK 517
C.1.1 ASSUMED BEHAVIOR IN A LEGACY ORIGINATING NETWORK 518
C.1.1.1 SS7 SIGNALING FROM ORIGINATING END OFFICE 518
C.1.1.2 MF SIGNALING FROM ORIGINATING END OFFICE 519
C.1.2 ASSUMED BEHAVIOR IN A SIP-BASED ORIGINATING NETWORK 520
C.2 BRIDGING CONSIDERATIONS 522
C.2.1 SIP AD HOC METHOD 523
C.2.2 ROUTE ALL CALLS VIA A CONFERENCE-AWARE UA METHOD 523
C.3 CALLED PARTY HOLD/SWITCH-HOOK STATUS 524
C.3.1 PROCEDURES AT THE LEGACY NETWORK GATEWAY 524
C.3.1.1 SS7 SIGNALING FROM ORIGINATING END OFFICE 524
C.3.1.2 MF SIGNALING FROM ORIGINATING END OFFICE 527
C.3.2 PROCEDURES AT THE ESRP 529
C.3.3 PROCEDURES AT THE I3 PSAP 530
C.3.4 PROCEDURES AT THE LEGACY PSAP GATEWAY 531
C.3.4.1 PROCEDURES AT THE LPG-NIF COMPONENT 531
C.3.4.2 PROCEDURES AT THE LPG-PIF COMPONENT 532
C.3.5 PROCEDURES AT THE BRIDGE 532
C.3.5.1 USING THE SIP AD-HOC METHOD 533
C.3.5.2 USING THE ROUTE ALL CALLS VIA A CONFERENCE-AWARE UA METHOD 533
C.4 RINGBACK 533

© Copyright 2011-2022 National Emergency Number Association, Inc.

C.4.1 PROCEDURES AT THE PSAP 533
C.4.2 PROCEDURES AT THE LEGACY PSAP GATEWAY 534
C.4.2.1 PROCEDURES AT THE LPG-PIF COMPONENT 534
C.4.2.2 PROCEDURES AT THE LPG-NIF COMPONENT 534
C.4.3 PROCEDURES AT THE ESRP 535
C.4.4 PROCEDURES AT THE LEGACY NETWORK GATEWAY 535
C.4.4.1 PROCEDURES AT THE LNG-NIF COMPONENT 535
C.4.4.2 PROCEDURES AT THE PIF COMPONENT 536
C.4.5 PROCEDURES AT THE BRIDGE 536
C.4.5.1 USING THE AD HOC METHOD 536
C.4.5.2 USING THE ROUTE ALL CALLS VIA A CONFERENCE-AWARE UA METHOD 537
C.5 ENHANCED CALLED PARTY HOLD 537
C.5.1 PROCEDURES AT THE LNG FOR CALLS RECEIVED OVER SS7 TRUNK GROUPS 538
C.5.1.1 PROCEDURES AT THE LNG-PIF COMPONENT 538
C.5.1.2 PROCEDURES AT THE LNG-NIF COMPONENT 538
C.5.2 PROCEDURES AT THE LNG FOR CALLS RECEIVED OVER MF TRUNK GROUPS 539
C.5.2.1 PROCEDURES AT THE LNG-PIF COMPONENT 539
C.5.2.2 PROCEDURES AT THE LNG-NIF COMPONENT 540
C.5.3 PROCEDURES AT THE BRIDGE 541
C.5.3.1 USING THE SIP AD HOC METHOD 541
C.5.3.2 USING THE ROUTE ALL CALLS VIA A CONFERENCE-AWARE UA METHOD 541
APPENDIX D – EXAMPLE CALL FLOWS (INFORMATIVE) 542
D.1 DATA BY VALUE SIP END-TO-END EXAMPLE CALL FLOW 542
D.1.1 STEP-BY-STEP DESCRIPTION 548
D.1.1.1 BOOT UP ACTIVITIES (STEPS NOT SHOWN) 548
D.1.1.2 PRE-CALL ACTIVITIES 548
D.1.1.3 CALL-RELATED ACTIVITIES 549
D.2 LOCATION BY REFERENCE / CELLULAR / HELD EXAMPLE CALL FLOW 560
D.2.1 STEP-BY-STEP DESCRIPTION 567
D.2.1.1 PROVISIONING ACTIVITIES (STEPS NOT SHOWN) 567
D.2.1.2 PRE-CALL ACTIVITIES 567
D.2.1.3 CALL-RELATED ACTIVITIES 567

© Copyright 2011-2022 National Emergency Number Association, Inc.

APPENDIX E - REST/JSON DEFINITIONS (NORMATIVE) 582
E.1 POLICY STORE 582
E.1.1 OPENAPI INTERFACE DESCRIPTION 582
E.1.2 EXAMPLES 601
E.2 DISCREPANCY REPORT 601
E.2.1 OPENAPI INTERFACE DESCRIPTION 601
E.2.2 EXAMPLES 617
E.3 DEQUEUE REGISTRATION 617
E.3.1 OPENAPI INTERFACE DESCRIPTION 617
E.4 MSAG CONVERSION SERVICE 619
E.4.1 OPENAPI INTERFACE DESCRIPTION 619
E.4.2 EXAMPLES 622
E.5 GEOCODE CONVERSION SERVICE 622
E.5.1 OPENAPI INTERFACE DESCRIPTION 622
E.5.2 EXAMPLES 624
E.6 TEST CALL 624
E.6.1 OPENAPI INTERFACE DESCRIPTION 624
E.6.2 EXAMPLES 627
E.7 ADDITIONAL DATA REPOSITORY 627
E.7.1 OPENAPI INTERFACE DESCRIPTION 627
E.7.2 EXAMPLES 629
E.8 LOGGING SERVICE 629
E.8.1 OPENAPI INTERFACE DESCRIPTION 629
E.8.2 EXAMPLES 657
E.9 BAD ACTOR SERVICE 657
E.9.1 OPENAPI INTERFACE DESCRIPTION 657
E.10 SERVICE/AGENCY LOCATOR SERVICE 659
E.10.1 OPENAPI INTERFACE DESCRIPTION 659
E.11 NOTIFY BODIES 664
E.11.1 ESRP NOTIFY NOTIFY BODY 664
E.11.1.1 JSON SCHEMA 664
E.11.1.2 GAP-OVERLAP NOTIFY BODY 665

© Copyright 2011-2022 National Emergency Number Association, Inc.

E.11.1.3 JSON SCHEMA 665
E.11.2 ABANDONED CALL NOTIFY BODY 666
E.11.2.1 JSON SCHEMA 666
E.11.3 ELEMENT STATE NOTIFY BODY 667
E.11.3.1 JSON SCHEMA 667
E.11.3.2 QUEUE STATE NOTIFY BODY 668
E.11.3.3 JSON SCHEMA 668
E.11.3.4 SERVICE STATE NOTIFY BODY 668
E.11.3.5 JSON SCHEMA 668
E.11.4 COMMON YAML 670
E.11.4.1 OPENAPI INTERFACE DESCRIPTION 670
ACKNOWLEDGEMENTS 672

© Copyright 2011-2022 National Emergency Number Association, Inc.

NENA
STANDARD DOCUMENT
NOTICE

This Standard Document (STA) is published by the National Emergency Number Association (NENA) as an information source for 9-1-1 System Service Providers, network interface vendors, system vendors, telecommunication service providers, and 9-1-1 Authorities. As an industry Standard it provides for interoperability among systems and services adopting and conforming to its specifications.

NENA reserves the right to revise this Standard Document for any reason including, but not limited to:

- Conformity with criteria or standards promulgated by various agencies,
- Utilization of advances in the state of the technical arts,
- Reflecting changes in the design of equipment, network interfaces, or services described herein.

This document is an information source for the voluntary use of communication centers. It is not intended to be a complete operational directive.

It is possible that certain advances in technology or changes in governmental regulations will precede these revisions. All NENA documents are subject to change as technology or other influencing factors change. Therefore, this NENA document should not be the only source of information used. NENA recommends that readers contact their 9-1-1 System Service Provider (9-1-1 SSP) representative to ensure compatibility with the 9-1-1 network, and their legal counsel, to ensure compliance with current regulations.

Patents may cover the specifications, techniques, or network interface/system characteristics disclosed herein. No license is granted, whether expressed or implied. This document shall not be construed as a suggestion to any manufacturer to modify or change any of its products, nor does this document represent any commitment by NENA, or any affiliate thereof, to purchase any product, whether or not it provides the described characteristics.

By using this document, the user agrees that NENA will have no liability for any consequential, incidental, special, or punitive damages arising from use of the document.

NENA's Committees have developed this document. Recommendations for changes to this document may be submitted to:

National Emergency Number Association
1700 Diagonal Rd, Suite 500
Alexandria, VA 22314
202.466.4911
or commleadership@nena.org

© Copyright 2011-2022 National Emergency Number Association, Inc.

NENA: The 9-1-1 Association improves 9-1-1 through research, standards development, training, education, outreach, and advocacy. Our vision is a public made safer and more secure through universally-available state-of-the-art 9-1-1 systems and better-trained 9-1-1 professionals. Learn more at nena.org.

Document Terminology

This section defines keywords, as they should be interpreted in NENA documents. The form of emphasis (UPPER CASE) shall be consistent and exclusive throughout the document. Any of these words used in lower case and not emphasized do not have special significance beyond normal usage.

1. MUST, SHALL, REQUIRED: These terms mean that the definition is a normative (absolute) requirement of the specification.
2. MUST NOT: This phrase, or the phrase "SHALL NOT", means that the definition is an absolute prohibition of the specification.
3. SHOULD: This word, or the adjective "RECOMMENDED", means that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
4. SHOULD NOT: This phrase, or the phrase "NOT RECOMMENDED" means that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.
5. MAY: This word, or the adjective "OPTIONAL", means that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item. An implementation which does not include a particular option "must" be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality. In the same vein an implementation which does include a particular option "must" be prepared to interoperate with another implementation which does not include the option (except, of course, for the feature the option provides.)

These definitions are based on IETF RFC 2119.

This document uses the word "call" to mean the following:

© Copyright 2011-2022 National Emergency Number Association, Inc.

1. A session established by signaling with two-way real-time media. This type of call usually involves a human making a request for help. This document sometimes uses "voice call", "video call", or "text call" when specific media is of primary importance. Real-time text and instant messaging using MSRP are examples of text calls of this type.
2. A one-time notification or series of data exchanges without media. A call of this type is referred to as a "non-interactive call". Such calls often do not involve a human at the calling end. Examples of non-interactive calls include a burglar alarm, an automatically detected HAZMAT spill, or a flooding sensor.

All types of calls are handled the same way.

The term "Incident" is used to refer to a real-world event for which one or more calls may be received.

The term Location Information Server (LIS) as listed in the NENA Master Glossary includes functions out of scope for i3. This document only uses those functions of a LIS described in Sections 3.2 and 4.10.

Intellectual Property Rights (IPR) Policy

NOTE – The user's attention is called to the possibility that compliance with this standard may require use of an invention covered by patent rights. By publication of this standard, NENA takes no position with respect to the validity of any such claim(s) or of any patent rights in connection therewith. If a patent holder has filed a statement of willingness to grant a license under these rights on reasonable and nondiscriminatory terms and conditions to applicants desiring to obtain such a license, then details may be obtained from NENA by contacting the Committee Resource Manager identified on NENA's website at www.nena.org/ipr.

Consistent with the NENA IPR Policy, available at www.nena.org/ipr, NENA invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard.

Please address the information to:

National Emergency Number Association
1700 Diagonal Rd, Suite 500
Alexandria, VA 22314
202.466.4911
or crm@nena.org

© Copyright 2011-2022 National Emergency Number Association, Inc.

Reason for Issue/Reissue

NENA reserves the right to modify this document. Upon revision, the reason(s) will be provided in the table below.

Document Number	Approval Date	Reason For Issue/Reissue
NENA 08-003	06/14/2011	Initial Document
NENA-STA-010.2-2016	09/10/2016	This document is issued to define a specification describing the functionality supported by elements associated with an ESInet and the interconnection of these functional elements. This second version of the Functional and Interface Standards for the NENA i3 Solution is intended to be used in Standards Development Organization (SDO) liaisons, and Request for Information (RFI)-like processes. It provides more detailed specifications for interfaces and functions, compared to the prior version and reflects experience with early implementations. The NENA i3 Architecture Working Group plans to release subsequent versions of the Standard as new work items are identified and resolved. Provide more detailed specification and reflect early implementation experience. Provisioning was taken out of scope and the section was removed.
NENA-STA-010.3-2021	07/12/2021	Major re-write. This version substantively modifies and provides additional specification to many sections of this document.
NENA-STA-010.3a-2021	10/07/2021	Publishing error corrections: Section 3.4.10.4.1, page 116, "nenaCallIncidentId" changed to "emergencyCallIncidentId". Section 4.7.1, page 208, escaped angle brackets (%3C, %3E) added to the example.
NENA-STA-010.3b-2021	11/30/2021	Publishing error corrections: 1) Section 3.3.3, page 74, corrected reference from E.10 to E.1.1 and clarifying that the

© Copyright 2011-2022 National Emergency Number Association, Inc.

Document Number	Approval Date	Reason For Issue/Reissue
		reference is to the 'Policy' type in Appendix E.1.1with rules conforming to the 'Rule' object. 2) Section 4.12.3.7 LogEventTypes specified that Elements that receive changes in ElementState MAY log receipt of such changes. The new state is logged with "StateChangeNotificationContents". This was not reflected in the YAML file as it should have been. This change fixes that error. 3) Appendix E.8.1 incorrectly provides additional IncidentId parameters in the IncidentMergeLogEvent, IncidentUnmergeLogEvent, IncidentSplitLogEvent, IncidentLinkLogEvent, and the IncidentUnlinkLogEvent. The extra parameters are deleted in the corrected YAML. 4) The text, in Section 4.12.3.7, specifies that the GatewayCallLogEvent must provide the pAni, if known. The YAML, in Section E.8.1, incorrectly lists the pANI type as "integer" when it should be "string". This change corrects that error.

2 General Concepts

2.1 Identifiers

To enable calls to be handled in an interconnected ESInet/NGCS, identifiers are standardized in the subsections below.

2.1.1 Agency Identifier

An Agency is represented by a fully qualified domain name (FQDN) as defined in RFC 2664 [229]. Each Agency MUST use one FQDN consistently in order to correlate actions across a

© Copyright 2011-2022 National Emergency Number Association, Inc.

wide range of calls and incidents. Any FQDN in the public Domain Name System (DNS) is acceptable as long as each distinct Agency uses a different FQDN. This ensures that each Agency Identifier (ID) is globally unique. An example of an Agency Identifier is "police.allegheny.pa.us". FQDNs can be represented with or without a final terminating dot (the final dot represents the DNS root). FQDNs are case-insensitive. FQDNs with and without a terminating dot MUST be treated as equivalent (e.g., "police.allegheny.pa.us." and "police.allegheny.pa.us" are equivalent).

2.1.2 Agent Identifier

An agent MUST be represented by an agent identifier that is a username, using the syntax for "Dot-string" in RFC 5321 [133] (that is, the user part of an email address, without the possibility of a "Quoted-String"). Usernames MUST be unique within the domain of the agency, which implies that the combination of Agent and Agency IDs is globally unique. Examples of this are "tom.jones@psap.allegheny.pa.us" and "tjones.atroop@state.vt.us".

2.1.3 Element Identifier

A logical name used to represent physical implementation of a functional element or set of functional elements as a single addressable unit (Section 2.11). The external interfaces of the element MUST adhere to the standards in this document. Elements are addressable via an FQDN that MUST be globally unique. An example of an Element Identifier is "esrp1.state.pa.us". Element Identifiers represent one instance of a replicated functional element when redundant instances of a function are provided for reliability.

2.1.4 URN Emergency Namespace

This document uses the "emergency" Namespace Identifier (NID) for Uniform Resource Name (URN) resources. Use of the "nena" NID is retained for backwards compatibility when used with v2 interfaces, but v3 interfaces MUST use the "emergency" NID. The lexical equivalence is the same as defined in *URN Syntax* (RFC 2141) [112]. Unless otherwise specified, all FEs MUST treat these URNs as case insensitive when doing comparisons in order to follow the lexical equivalency rules of *A Uniform Resource Name (URN) for Emergency and Other Well-Known Services* (RFC 5031) [45].

2.1.5 Services

A set of functional element instances that provide the basic capabilities described in this document is called a Service. Services defined in this document are known by a Service Name which comes from the Service Name registry (Section 10.11).

A service can be implemented in one or more elements, and indeed for redundancy purposes, nearly every service SHOULD be implemented by multiple elements. Regardless,

© Copyright 2011-2022 National Emergency Number Association, Inc.

the external interfaces of the service MUST adhere to the standards in this document. A Service Identifier refers to the collection of elements that define a service within an NGCS. Service Identifiers are Fully Qualified Domain Names (FQDNs). An example of a Service Identifier is "foo.allegheny.pa.us". The Service Name is not required to be part of the FQDN.

2.1.6 Call Identifier

The term "call" is defined in Document Terminology and includes voice calls, video calls, text calls, and non-interactive calls. The first element in the first ESInet/NGCS that handles a call assigns the Call Identifier. The form of a Call Identifier is a Uniform Resource Name (URN) (RFC 2141) [112] formed by the prefix "urn:emergency:uid:callid:", a unique string containing alpha and/or numeric characters, the ":" character, and the Element Identifier of the element that first handled the call. For example, "urn:emergency:uid:callid:a56e556d871:bcf.state.pa.us" is a properly formatted Call Identifier. The unique string portion of the Call Identifier MUST be unique for each call the element handles over time. The length of the unique string portion of the Call Identifier MUST be a string of 10 to 32 characters. One way to create this unique string is to use a timestamp with a suffix that differentiates multiple calls if they could be created by the element in the same instant. Implementations using multiple physical devices to implement a redundant element MAY need an additional component to guarantee uniqueness. The Call Identifier is added to a Session Initiation Protocol (SIP) message using a Call-Info header field with a purpose of "emergency-CallId". For example:

```
Call-Info: <urn:emergency:uid:callid:a56e556d871:bcf.state.pa.us>;
purpose=emergency-CallId
```

Every call, including non-emergency calls, MUST have a unique Call Identifier.

2.1.7 Incident Tracking Identifier

A real-world event such as a heart attack, car crash, or a building fire for which one or more calls may be received is an Incident. Examples include a traffic accident (including subsequent secondary crashes), a hazardous material spill, etc. Multiple Calls MAY be associated with an Incident. An Incident MAY include other Incidents in a hierarchical fashion. The form of an Incident Tracking Identifier is a URN formed by the prefix "urn:emergency:uid:incidentid:", a unique string containing alpha and/or numeric characters, the ":" character, and the Element Identifier of the entity that first declared the incident. For example, "urn:emergency:uid:incidentid:a56e556d871:bcf.state.pa.us" is a properly formatted Incident Tracking Identifier. The string MUST be unique for each Incident the element handles over time. The length of the unique string portion of the Incident Tracking Identifier MUST be a string of 10 to 32 characters. One way to create this unique string is to use a timestamp with a suffix that differentiates multiple Incidents if

© Copyright 2011-2022 National Emergency Number Association, Inc.

they could be created by an element in the same instant. Implementations using multiple physical devices to implement a redundant element MAY need an additional component to guarantee uniqueness. Incident Tracking Identifiers are globally unique. By definition, there is an Incident associated with every emergency call. As a practical matter, there is at least one call associated with every Incident, except those incidents declared by an agent (such as a police officer observing a traffic incident). The Incident Tracking Identifier is locally generated and assigned by an LNG, LSRG, or the first element in the first ESInet/NGCS that handles an emergency call or declares an incident. Incident Tracking Identifiers MAY be assigned to a call prior to determining the real-world incident to which it actually belongs. (See Section 4.2.2.2). The Incident Tracking Identifier MUST be added to a SIP message using a Call-Info header field with a purpose of "emergency-IncidentId". For example:

```
Call-Info: <urn:emergency:uid:incidentid:a56e556d871:bcf.state.pa.us>;
purpose=emergency-IncidentId
```

2.1.8 LogEvent Identifier

Each Logging Service MUST assign a globally unique identifier to each LogEvent. The form of a LogEvent Identifier is a URI consisting of the string "urn:emergency:uid:logid:", a unique string, the ":" character, and the FQDN of the Logging Service. The unique string MUST be 10 to 36 characters long and unique to the Logging Service. An example LogEvent Identifier is "urn:emergency:uid:logid:0013344556677-231:logger.state.pa.us". The FQDN specified MUST be the domain of the Logging Service to which a corresponding RetrieveLogEvent request can be sent to access the LogEvent.

2.1.9 Queue Identifier

The Queue Identifier, which is represented by a URI, MUST have the domain part of the URI set to the domain in which the queue (the destination for calls) resides (ESRP or PSAP, for example). An example of a PSAP URI is normalCalls@psap.allegheny.pa.us.

2.1.10 Secure Telephone Identity

The Secure Telephone Identity is defined as the identity provided in a SIP Identity header field, constructed and formatted as per RFC 8224 [60]. When present, it is used to validate the identity of the calling party.

2.2 Time

It is essential that all elements on the ESInet/NGCS have the same notion of time. To do so, every element MUST implement Network Time Protocol (NTP) (RFC 5905) [216], and access to a hardware clock MUST be provided in each ESInet/NGCS such that the absolute

© Copyright 2011-2022 National Emergency Number Association, Inc.

time difference between any element on any ESInet/NGCS and another element in the same or any other ESInet/NGCS is maintained within one tenth of a second[3] of one another. (See Section 4.17).

2.3 Timestamp

Any record that must be marked as to when it occurred (especially a log record, see Section 4.12) includes a Timestamp. A Timestamp includes integer-valued year, month, day, hour, minute, seconds, a decimal seconds value, and a timezone offset value. Time MUST include seconds, and, if two or more Timestamps could be generated by the same element within one second when the order of events matters, the seconds element MUST include sufficient decimal places in the seconds field to differentiate the Timestamps. Except when otherwise dictated by standards, all time within the ESInet/NGCS is represented as local time with offset from Universal Coordinated Time (UTC). The offset MUST be based on the local time of the creator. The offset is a REQUIRED component of the Timestamp and consists of an integer number of hours and minutes.

Timestamps contained in JavaScript Object Notation (JSON) objects governed by this specification SHALL be represented by the "date-time" datatype described in RFC 3339, Section 5.6 [135], and SHALL be indicated in schema definitions accordingly. An example of a Timestamp in this format is "2015-08-21T12:58:03.01-05:00".

2.4 Events Common to Multiple Functional Elements

Events are described in Section 3.1.3.2. The following events MAY be implemented in any functional element. Also see the Logging Service interface in Section 4.12, which is implemented by any element that handles a call.

2.4.1 Element State

The elementState event package provides the state of an element either determined automatically or as determined by management. A registry (ElementState) of allowed values is defined (see Section 10.13).

In addition, if the subscriber to an element is unable to contact that element, it MUST assume the state of the element is "Unreachable".

A physical or virtual implementation that is separately addressable or differentiable between other entities of the same type MUST implement elementState.

[3] Some implementations MAY require more time accuracy than this specification within a domain such as an ESInet/NGCS.

© Copyright 2011-2022 National Emergency Number Association, Inc.

Event Package Name: emergency-ElementState

Event Package Parameters: None

SUBSCRIBE Bodies: Standard RFC 4661 [92] + extensions filter specification MAY be present

Subscription Duration: Default is one (1) hour. One (1) minute to 24 hours is reasonable.

NOTIFY Bodies: MIME type Application/EmergencyCallData.ElementState+json

Name	Condition	Description
elementId	MANDATORY	Element identifier
state	MANDATORY	Enumeration of current state from Internet Assigned Numbers Authority (IANA) ElementState registry
reason	OPTIONAL	Text containing the reason state was changed, if available

Notifier Processing of SUBSCRIBE Requests

The notifier consults the policy (elementState) specifying the Element Identifier as the target to determine if the requester is permitted to subscribe. It returns 603 (Decline) if not acceptable. If the request is acceptable, it returns 200 OK. Notifiers MUST implement event rate filters as described in RFC 6446 [80].

Notifier Generation of NOTIFY Requests

When the state of the element changes, a new NOTIFY request is generated, adhering to the filter requests. Filter requests MAY specify a minimum notification interval. The element MUST generate a NOTIFY meeting this filter, if specified. This can be used as a watchdog mechanism.

Subscriber Processing of NOTIFY Requests

No specific action required.

Handling of Forked Requests

Forking between elements MUST NOT be used.

Rate of Notification

© Copyright 2011-2022 National Emergency Number Association, Inc.

State normally does not change often. Changes MAY occur every few seconds if the network or systems are unstable. A minimal rate should be used to ascertain a subscription is still valid.

State Agents

No special handling is required.

2.4.2 Service State

The serviceState event indicates the state of a service either automatically determined, or as determined by management. It encompasses the state of the designated service, inclusive of its security posture when supported. The Request-URI of the SUBSCRIBE specifies the Service Identifier of the target Service.

Two IANA registries of allowed values are defined, one for "serviceState" (see Section 10.12) and one for "securityPosture" (see Section 10.18).

In addition, if the subscriber to a service is unable to contact that service, it MUST assume the state of the service is "Unreachable".

Note that one or more elements MAY implement one or more service(s). Each addressable element would have its own element state; each service would have an independent service state.

Event Package Name: emergency-ServiceState

Event Package Parameters: None

SUBSCRIBE Bodies: Standard RFC 4661 [92] + extensions filter specification MAY be present

Subscription Duration: Default 1 hour. 1 minute to 24 hours is reasonable.

NOTIFY Bodies: MIME type Application/EmergencyCallData.ServiceState+json

Name	Condition	Description
service	MANDATORY	Service subscribed to
name	MANDATORY	Name of the service. Enumeration of current service name from the IANA service registry
serviceId	MANDATORY	Service Identifier
serviceState	MANDATORY	

© Copyright 2011-2022 National Emergency Number Association, Inc.

Name	Condition	Description
state	MANDATORY	Enumeration of current state from the IANA serviceState registry
reason	MANDATORY	Text containing the reason state was changed, if available. Otherwise, empty
securityPosture	CONDITIONAL If the service maintains Security Posture, the field MUST be present. Otherwise, it is omitted.	
posture	MANDATORY	Mandatory if the securityPosture field is present. Enumeration of current security posture from the IANA securityPosture registry
reason	OPTIONAL	Text containing the reason posture changed, if available. Otherwise, empty.

Notifier Processing of SUBSCRIBE Requests

The notifier consults the policy (serviceState) specifying the ServiceIdentifier as the target to determine if the requester is permitted to subscribe. It returns 603 (Decline) if not acceptable. If the request is acceptable, it returns 200 OK. Notifiers MUST implement event rate filters, RFC 6446 [80].

Notifier Generation of NOTIFY Requests

When the state of the service changes, a new NOTIFY request is generated, adhering to the filter requests. Filter requests MAY specify a minimum notification interval. The element MUST generate a NOTIFY meeting this filter, if specified. This can be used as a watchdog mechanism.

Subscriber Processing of NOTIFY Requests

No specific action required.

Handling of Forked Requests

Forking between elements MUST NOT be used.

© Copyright 2011-2022 National Emergency Number Association, Inc.

Rate of Notification

State normally does not change often. Changes MAY occur every few seconds if the network or systems are unstable.

State Agents

No special handling is required.

2.5 Location Representation

Location in NG9-1-1 is represented by content in a PIDF-LO[4] document (RFC 4119 [6], updated by RFC 5139 [53] and RFC 5491 [52]) with field use for the United States as documented in the NENA Civic Location Data eXchange Format (CLDXF) [77]. An equivalent definition for Canadian addresses will be referenced in a future version of this document. Fields in the PIDF-LO must be used as defined; no local variation is permitted. A function (PIDFLOtoMSAG) is provided as part of the MSAG Conversion Service (See Section 4.4) for translating PIDF-LO to a NENA-standard MSAG representation for backwards compatibility. Geodetic location MUST be one of the shape listed in [69]. All geodetic data in i3 uses WGS84 as the datum.

A PIDF-LO has an element called "retransmission-allowed", which, when missing or set to false, is meant to prohibit forwarding of the PIDF-LO. Handling of location when processing an emergency call is controlled by law, and NG9-1-1 FEs normally would ignore retransmission-allowed within the ESInet/NGCS for such calls. There are circumstances in which data about an emergency call may be sent to entities not covered by existing law. In those circumstances it is desirable that NG9-1-1 FEs honor the privacy wishes of the sender as expressed in the retransmission-allowed field. FEs SHOULD honor the "retransmission-allowed" element of the PIDF-LO when laws do not specify privacy is suspended. When laws suspend privacy, FEs SHOULD send location regardless of the value of the "retransmission-allowed" element. When handling non-emergency calls, retransmission-allowed SHOULD be honored.

An entity conforming to this specification that supplies a PIDF-LO for an emergency call MUST use the <provided-by> element to convey its Data Provider Additional Data block, as specified in RFC 7852 [107] Section 4.1. Note that the PIDF-LO supplier's Data Provider block MUST also be conveyed using a Call-Info header field as described in sections 3.1.15

[4] In the IETF, location information (Location Object) is a subset of Presence information (Presence Information Data Format): PIDF-LO. While NG9-1-1 uses PIDF and the IETF mechanisms that are described in the Presence service, no other parts of Presence are used in emergency calls although Presence may be used in other parts of NG9-1-1.

© Copyright 2011-2022 National Emergency Number Association, Inc.

and 4.11, unless the supplier is not in the call path. The <provided-by> element MUST NOT be used to convey any other Additional Data blocks. The "dataProvider" schema [ref3] of the "pidf:geopriv10:dataProvider namespace" [ref4] MUST NOT be used. It is RECOMMENDED that the Data Provider Additional Data block be conveyed by value rather than by reference, to avoid an additional operation to obtain the data.

2.6 xCard/jCard

In many interfaces defined in this and related NG9-1-1 documents, a common need is to provide contact information. For example, in some blocks of Additional Data and in Service/Agency Locator, the identity and contact information is part of the data structure. When contact data is needed, i3 specifies the use of an xCard in eXtensible Markup Language (XML) format per RFC 6351 [113] where the interface must be XML, and a jCard as defined in RFC 7095 [215] when the interface is JSON.

2.7 Emergency Services IP Networks

ESInets are private, managed, and routed IP networks. An ESInet serves a set of PSAPs, a region, a state/province, or a set of states/provinces. ESInets are interconnected to neighboring ESInets so that traffic can be routed from any point in the ESInet to any point in any other ESInet. States/Provinces MAY have a backbone ESInet either directly connecting to all PSAPs in the state/province, or interconnected to all county/parish or regional ESInets. Neighboring states/provinces or regions SHOULD interconnect their ESInets. It is desirable to have a backbone national ESInet in each country to optimize routing of traffic between distant ESInets. Each PSAP MUST be connected to an ESInet, possibly through a Legacy PSAP Gateway.

ESInets MUST accept and route IPv4 and IPv6 packets. All services MUST support IPv4 and IPv6 interfaces. IPv6 is RECOMMENDED for use throughout the ESInet, but cannot be assumed. Within this document there are several interfaces that may require a text representation of an IPv6 address, including in the specification of addresses for media in the Session Description Protocol (SDP). In such interfaces the canonical representation specified in RFC 5952 [196] MUST be used, including the use of brackets when specifying a port number. Note that originating networks are outside the scope of this document and they may not follow RFC 5952 conventions.

ESInets MUST be accessible from the global Internet, with calls going through the Border Control Function (BCF). This Internet interconnect is RECOMMENDED at the state ESInet level with local or regional ESInets getting Internet connectivity via the state ESInet. Originating networks SHOULD be connected to any ESInet to which they regularly deliver volume traffic via a private connection through the BCF of that ESInet.

© Copyright 2011-2022 National Emergency Number Association, Inc.

An ESInet MUST be capable of withstanding the largest feasible Distributed Denial of Service (DDoS)/Telephone Denial of Service (TDoS) attack. As of this version, that means approximately at least a terabit of mitigation. Network and BCF bandwidth as well as mitigation services may be used to achieve this requirement. DDoS/TDoS mitigation typically requires that traffic be rerouted to a mitigation service. Private connections MUST be able to be so re-routed if mitigation is needed. Connection through the Internet is acceptable, PREFERABLY through a Virtual Private Network (VPN) with the same mitigation caveat.

Note: The effect on emergency calls already in progress when mitigation is enabled will be addressed in a future version of this document.

Access to ESInets MUST be controlled. Only public safety agencies and their service providers may be connected directly to the ESInet. Call origination sources, gateways, and similar elements are outside the ESInet and interconnected through the BCF. However, for security reasons, the ESInet SHOULD NOT be assumed to be a "walled garden."

For Quality of Service (QoS) reasons, IP traffic within an ESInet MUST implement DiffServ (RFC 2474 [218] and 2475 [134]). Differentiated Service Code Points (DSCPs) within the ESInet are drawn from pool 2, with the exception of DSCP value "0000 00" which is the default from Pool 1. Routers MUST respect code points: Functional Elements MUST mark packets they create with appropriate code points. The ESInet edge router MUST perform traffic conditioning for packets entering the ESInet. The following code points MUST be used, so that packets transiting more than one ESInet can receive appropriate treatment. The following Per Hop Behaviors (PHB) on ESInets are RECOMMENDED starting points and MAY be changed based on operational experience:

This table specifies ESInet-specific traffic. Other traffic (e.g., DHCP, ICMP, BGP, etc.) should be marked according to industry standards and best practices.

DSCP	Use	PHB
0000 00	Routine Traffic except as specified below	Default (Best Effort)
0000 11	9-1-1 Call (SIP) Signaling (including non-interactive calls) and emergency call related HTTP/S operations, DNS traffic	AF12
0001 11	9-1-1 Text Media (RTT and MSRP)	AF12
0010 11	9-1-1 Audio Media (9-1-1 Calls and admin calls)	EF
0011 11	9-1-1 Video Media	AF11

Interconnected ESInets represent a DS Region as defined in RFC 2475 [134] and connect to other networks which are distinct DS Regions. The ESInet edge routers SHOULD re-mark code points between the interconnected networks and the ESInet to match the traffic classes ("Use") above as closely as possible, within the terms of any interconnect

© Copyright 2011-2022 National Emergency Number Association, Inc.

agreements with such networks. An interconnected network might perform the re-marking at its edge routers, in which case the ESInet edge router's re-marking is a null operation.

All elements in an ESInet SHOULD have a publicly addressable IP address. Network Address Translations (NATs) SHOULD NOT be used within an ESInet. Although NAT use within an ESInet is NOT RECOMMENDED, NATs may be needed in specific deployments, and therefore all network elements MUST operate in the presence of NATs.

It is RECOMMENDED that elements connected to the ESInet not be referred to by their IP address but rather through a hostname using DNS. Use of statically assigned IP addresses SHOULD be limited, and SHOULD NOT be used with IPv6 addresses. Dynamic Host Configuration Protocol (DHCP) (RFC 2131) [147] or Dynamic Host Configuration Protocol for IPv6 (DHCPv6, RFC 8415 [233]) must be implemented on all network elements to obtain IP address, gateway, and other services.

There SHALL NOT be any single point of failure for any critical service or function hosted on the ESInet. Certain services designated as non-critical may be exempt from this requirement. These MUST NOT include the BCF, internal ECRF, ESRP, Logging Service, and security services. Services MUST be deployed to survive disasters, deliberate attacks, and massive failures.

2.8 Service Interfaces

In this document, we make use of three kinds of interfaces:

- Web Services, typically using a Simple Object Access Protocol (SOAP) [148] interface or using Representational State Transfer (REST),
- Simple HyperText Transfer Protocol Secure (HTTPS) (RFC 2818) [153] GET (and in some cases, POST) with retrieval of JSON data structures based on a Uniform Resource Identifier (URI), and
- SIP interfaces, including SIP Subscribe/Notify.

The term "web service", when it appears in this document, unless otherwise specified as an IETF-defined XML interface, means a REST interface using JavaScript Object Notation (JSON) defined by a NENA-provided Open API 3.0 YAML (YAML Ain't Markup Language) file (Appendix E.).

The interface point for web services MUST be the server line of the YAML file, with the Service Identifier of the appropriate service substituted for "localhost".

The YAML file in Appendix E represents the normative definition of the interface; if there are any discrepancies between the YAML file in the repository and the YAML file in the text (Appendix E), the YAML file in the repository is authoritative.

© Copyright 2011-2022 National Emergency Number Association, Inc.

2.8.1 HTTP Transport

i3 Services which use HTTP MUST support HTTP over TLS (HTTPS) (RFC 2818) [57]. The services, unless specified otherwise, MUST support HTTP/1.1 (RFC 7230) [162] and SHOULD support HTTP/2.0 (RFC 7540) [197]. Clients and servers MUST support TLS 1.2 [199], MAY support TLS 1.3 [200] or greater and MUST NOT offer or accept TLS 1.1 or TLS 1.0. Perfect forward secrecy MUST be used within the ESInet.

2.8.2 Status Codes

Each entry point lists status codes that are returned for expected situations. (For example, Section 4.12.3.1.1 LogEvent response includes the codes 200 OK, 434 Signature Verification Failure, and 463 LogEvent extension on disallowed list, as well as other codes.) In some cases, an IANA-registered [222] status code is used (e.g., 200 OK in the above), while in other cases, custom status codes are used (e.g., 434 Signature Verification Failure and 463 LogEvent extension on disallowed list in the above). If a server encounters a situation not listed, the most appropriate IANA-registered status code SHOULD be used (for example, 500 Internal Server Error for a server fault or 507 Insufficient Storage if a server is unable to store a resource).

Clients MUST appropriately handle all status codes listed for each supported entry point, and MUST react appropriately to other status codes received, based on the first digit as per RFC 7231 [223] Section 6.

2.8.3 Versions

Each web service has a version. A version consists of a major version and a minor version, both integers. Versions are commonly expressed as a string with a period between the major and minor version integers (e.g., "3.2"). The integer before the period represents the major version, and the integer after the period represent the minor version. Any change to the YAML file will change the version. If a set of changes to the YAML file is backwards compatible, the minor version is incremented. If any of a set of changes to the YAML file is not backwards compatible, the major version is incremented, and the minor version reset to zero. Implementations MUST ignore elements of data structures they do not understand and MUST return 404 errors to entry points to the web interfaces they don't provide as a server. If a minor version introduces a backwards compatible change that is not accommodated by existing implementations of the same major version solely by ignoring elements it doesn't understand and returning 404 errors for entry points it doesn't understand, the document describing the new minor version MUST describe precisely how implementations of that and succeeding minor versions accommodate prior minor versions. Other NENA standards MAY specify changes to the interface, and thus the version.

© Copyright 2011-2022 National Emergency Number Association, Inc.

Changes that are not backwards-compatible changes SHOULD only be made in future version of this document.

Each Web Service MUST implement an entry point called "Versions". For example, the PolicyStore web service implements .../PolicyStore/Versions. Clients of Web Services MUST make an HTTPS GET request using the URI of the service's Versions entry point. The GET does not have any parameters. The server sends a response containing a data structure to inform the client which versions the server supports. The "Versions" entry point returns the following parameters:

Name	Condition	Description
fingerprint	MANDATORY	Vendor Info
versions	MANDATORY	One entry for each version supported at the server

Status Codes
200 OK Version information returned

"versions" contains an array of objects, each consisting of:

Name	Condition	Description
major	Mandatory	Major version number
minor	Mandatory	Minor version number
vendor	Optional	Vendor extensions
serviceInfo	Conditional: required for services that specify this parameter, omitted for all others	Service-specific information. Some web services return additional service-specific information; for such services, this parameter is present and contains additional parameters as specified for the service; for services that do not specify the use of this parameter, it is omitted.

The "vendor" string is not defined in this version of the document but is intended to indicate which vendor extensions the implementation supports.

The "fingerprint" string is intended to contain a unique string for a particular code set (e.g., a build identifier). The string is logged (in the "VersionsEvent" LogEvent) for debugging purposes but is otherwise not used.

The Versions entry point MAY be used as a keep-alive mechanism for a service. Successful queries for this purpose SHOULD NOT be logged by the client. When a change in version is detected, however, this SHOULD be logged by the client.

© Copyright 2011-2022 National Emergency Number Association, Inc.

Note that the information returned by the Versions entry point can be different for different Web Services even if the IP addresses of the servers are the same, and that version information can change between requests (e.g., a server could fail-over).

For example, assuming a hypothetical Web Service "Tantrums" that specifies a "maxScreamVolume" parameter in serviceInfo, an HTTPS GET request on …/Tantrums/Versions" returns a body containing a JSON data object similar to the following:

```
{
   "fingerprint": "Woof-FurrySuite-v8-8c439e",
   "versions":
       [
          { "major": 6, "minor": 3,
            "vendor": "burby-magic",
            "serviceInfo": { "maxScreamVolume": 11 }
          }
       ]
}
```

2.9 Redundancy

Many methods are available to implementers to create reliable implementations. Some methods require clients to be aware of the redundancy model of the server in order to achieve the desired reliability model. Interoperability is affected if there is a mismatch in what the client assumes and what the server (or peer) assumes with respect to redundancy.

The i3 architecture provides support for one model in which clients expressly support two (or optionally more) servers in an active-active (multi-master) configuration. Each client must be prepared to send its transactions to one of two (or optionally more) servers. One interface is considered "primary" with "secondary" interface(s) available to be used at any time by any client. Deployment of this mechanism is not a requirement.

Servers may implement other models as long as it is transparent to the client. If the server has a redundancy model that hides redundancy from the client, only the primary interfaces would be used. This model does not support an active/standby failover paradigm – it is active-active. The burden of maintaining consistency of transactions when replicated databases are used rests on the server. Clients MUST retry transactions on redundant elements that that could not be completed on the initial element.

Every implementation MUST be capable of using a DNS based implementation of redundant elements where more than one address may be returned for the URI provided. Implementations MUST be capable of preferring the first returned address, and using the second, third and optionally additional addresses returned as representing redundant

© Copyright 2011-2022 National Emergency Number Association, Inc.

elements for the service. Other mechanisms to achieve redundancy MAY be provided, but the DNS based mechanism MUST be supported by all services and clients of those services.

Examples of how an active-active architecture is implemented at the server are beyond the scope of this document.

2.10 Telephone Numbers

When telephone numbers are used within the NGCS, full E.164 [120] numbers may be encountered on any call and all elements MUST be able to handle a full E.164 telephone number. Ten-digit numbers conforming to the North American Numbering Plan (NANP) may be assumed to be North American telephone numbers and telephone numbers that are not full E.164 numbers but contain a digit string with greater than 10 digits may be assumed to be non-North American telephone numbers, but missing the "+" prefix. Some systems may have more sophisticated methods of determining a full E.164 number from a digit sequence appearing in the signaling. Telephone numbers conveyed as part of a URI MUST be designated as such either by using a tel URI (RFC 3966) [150] or in a SIP URI using the user=phone parameter. SIP elements MUST conform to RFC 3824 [29]

2.11 Functional Elements

This document describes many functional elements. An implementation MAY combine any set of functional elements into a physical realization, provided that the assembly of functional elements provides all of the required functionality specified in this standard, as well as the external interfaces that the set of elements offer to other ESInet/NGCS elements. Interfaces between the FEs within a physical realization do not have to conform to the interfaces described in this document, provided that the set of elements behaves as if those interfaces conformed to this document.

3 Interfaces

This section describes the major interfaces used in NG9-1-1. Not every interface is described in this section; some of the web interfaces, for example, the Additional Data dereferencing interfaces, are described in other documents or in other sections of this document.

3.1 SIP Call

The i3 call interface is SIP (RFC 3261) [10]. All calls presented to the NGCS MUST be SIP signaled. Calls are potentially multimedia, and can include one or more forms of media

© Copyright 2011-2022 National Emergency Number Association, Inc.

(audio, video, and/or text[5]). See Section 3.1.11 for a discussion of "non-interactive calls" (also called "data-only emergency calls") which are used for requests for help when there is no human caller. SIP MUST also be the protocol used to call a 9-1-1 caller back, and is the protocol for calls between agents within the ESInet.

SIP is a complex protocol defined in a large number of standards documents. All NG9-1-1 elements which process calls MUST implement all of the standards listed in Section 3 (Core Standards) of the "Hitchhiker's Guide to SIP" (RFC 5411) [9], and RFC 4320 [36]. Implementations are cautioned to be "strict in what you send, and liberal in what you accept" with respect to such standards. It is generally unacceptable to drop a 9-1-1 call just because it doesn't meet some standard detail if it's reasonably possible to process the call anyway. This section does not describe a change to any normative text in any IETF standards-track document. If there is any conflict between this document and the IETF document concerning how the SIP protocol works, the IETF document is authoritative. Many elements of SIP have options, and this document may restrict an implementation's use of such options within an ESInet.

Note: There are some conflicts between some of the documents mentioned in RFC 5411 and this document. This will be addressed in a future version of this document.

There are three primary entities in a SIP protocol exchange:

1. The User Agent Client (UAC), which is the initiator of a "transaction" within SIP. In the origination of a 9-1-1 call, the calling party's end device could be the UAC.
2. The User Agent Server (UAS), which is the target of a transaction within SIP. In the origination of a 9-1-1 call, the call taker's end device could be the UAS.
3. A Proxy Server, which is an intermediary that assists in the routing of a call. Proxy servers are in the signaling path of a call, but not in the media path. A call may traverse several proxies. In a typical 9-1-1 call, the calling party's originating network may have two or more proxies. The NGCS has at least one proxy (an Emergency Service Routing Proxy) and typically has more than one.

In addition, some implementations may make use of a Back-to-Back User Agent (B2BUA) which is an interconnected UAC and UAS.

SIP message exchanges are defined in transactions, which are explicit sequences of messages. The transaction is named by the "method" in the SIP message that starts the

[5] All ESInet elements support all forms of media described in this document. Any given originating network or device may not support all media types, and support of specific media types by originating networks and devices may be subject to regulation.

© Copyright 2011-2022 National Emergency Number Association, Inc.

transaction. For example, the SIP transaction that creates a call (termed a "session" in SIP) is the INVITE transaction.

In this document, we use the terms "diversion" and "retarget" to mean that a call is sent to a PSAP other than the nominal PSAP, normally due to unusual conditions at the nominal PSAP. In SIP, these terms are used for behaviors with strict definitions that generally involve a change in the Request-URI. However, because emergency calls maintain a service urn in the Request-URI, changes in the destination are accomplished via the Route header.

Forking between elements MUST NOT be used.

Emergency call handling relies on the Service URN in the Request-URI being preserved. To avoid the Request-URI being rewritten, this document assumes loose routing (as defined in RFC 3261 [10]) is used for all SIP Calls end-to-end. Per RFC 3261, the "lr" parameter should be present in URIs used for routing. A future version of this document will normatively require this behavior.

Complete emergency call examples are presented in Appendix D.

3.1.1 Minimal Methods needed to handle a call

The only SIP methods absolutely REQUIRED to handle a 9-1-1 call are the INVITE (for interactive calls) or MESSAGE (for non-interactive calls). The REFER method (defined in RFC 3515 [19]) MUST also be supported in order to conference and transfer calls. Call takers (and thus bridges that they may use) MUST be able to generate the BYE transaction to terminate the call.

NG9-1-1 elements that process 9-1-1 calls MUST accept calls that do not strictly follow the SIP standards. As long as the messages can be parsed, and the method discerned, at least the first SIP element (the BCF) MUST be able to accept the call and forward the call onward (see Section 4.1), possibly rewriting non-conforming signaling messages. There are security concerns with accepting non-conforming calls; the BCF MAY reject calls that appear to be security risks.

Support for the following SIP Methods is summarized and specified in the following table:

SIP Method	Mandatory/Must Not/ Conditional/Optional
INVITE	MANDATORY
REFER	MANDATORY
BYE	MANDATORY
CANCEL	MANDATORY
UPDATE	MANDATORY
OPTIONS	MANDATORY
ACK	MANDATORY

© Copyright 2011-2022 National Emergency Number Association, Inc.

SIP Method	Mandatory/Must Not/ Conditional/Optional
PRACK	MANDATORY
MESSAGE	MANDATORY
INFO	MANDATORY (But must not be used to convey DTMF digits)
REGISTER	MUST NOT
SUBSCRIBE/NOTIFY	MANDATORY
PUBLISH	OPTIONAL

3.1.1.1 INVITE (initial call)

The INVITE method is used to initiate an interactive call. The standard INVITE/200 OK/ACK sequence MUST be followed, with allowance for provisional (1XX) responses.

An emergency call has a Route header field containing next-hop data obtained from the ECRF (which should be augmented with the "lr" parameter to avoid Request-URI) rewriting based on the location of the call, and a Request-URI containing a Service URN. Nominally, the Service URN SHOULD be "urn:service:sos" or a subservice. In most jurisdictions, subservices such as "urn:service:sos.police", "urn:service:sos.fire" and "urn:service:sos.ambulance" appearing on a call presented to the Next Generation 9-1-1 Core Services (NGCS) are routed as they would be without the subservice.

The external (i.e., facing outside the ESInet/NGCS) ECRF returns a "PSAP URI" which is contained in the Route header field (which should be augmented with the "lr" parameter to avoid Request-URI rewriting) when the call enters the ESInet/NGCS. The content of this URI can vary depending on the policy of the 9-1-1 Authority. One strategy is simply to use a general URI that leads to a state level ESRP, for example "911@sos.tx.us". The state ESRP queries the internal ECRF (within the ESInet/NGCS) with the service URN found in the PRF policy for the incoming call, for example "urn:emergency:service:sos.psap", and receives the next hop route for the call. Alternatively, the external ECRF could return a more specific URI, for example, "harris.county@sos.tx.us". This URI still routes to the same state-level ESRP, which performs the same ECRF query. However, failures at the state ESRP (for example, a failure to obtain a route from the ECRF) may be able to be mitigated by using the information in the Route header field.

Every call received by the NGCS gets some form of "call treatment". Minimal call treatments defined include:

1. Route call to the PSAP serving the location of the caller
2. Return Busy (600 Busy Everywhere)
3. Answer at an Interactive Media Response (IMR) system
4. Divert to another PSAP

© Copyright 2011-2022 National Emergency Number Association, Inc.

The ESRP determines, by evaluating PSAP policies, which treatment a call gets.

An i3 PSAP SHOULD normally only return a 180 Ringing provisional response when a 9-1-1 call is queued for answer. 183 Session Progress may be used in some specific circumstances. It is RECOMMENDED that no other 1XX response be used by the i3 PSAP due to uneven implementations of these responses. The provisional response SHOULD be repeated at approximately 3 second intervals if the call is not answered. When placing a call-back, elements MUST accept any 1XX intermediate response and provide an appropriate indication to the caller.

The normal response to an answered call is 200 OK.

9-1-1 calls are usually not redirected, and thus 3XX responses are normally not used; however, 3XX MAY be used for calls initiated within the ESInet/NGCS. If a call is retargeted, History-Info and Reason header fields MUST be added to the INVITE/MESSAGE per section 3.1.8. NG9-1-1 elements that initiate calls within the ESInet/NGCS SHOULD appropriately respond as defined in RFC 3261 [10].

Once a call is established, it may be necessary to modify some of the parameters of the call. For example, it may be necessary to change the media session parameters. In this case, an INVITE transaction on an existing session is used. This is termed a "re-INVITE" in SIP. A re-INVITE MAY be used on any call within the ESInet/NGCS, including a 9-1-1 call. A re-INVITE MAY be initiated from either end of the call. Note that when the called party initiates the re-INVITE it becomes the UAC, and the calling party becomes the UAS. A party MUST be able to accept a re-INVITE which changes the Contact header field. This may occur in the case of an element failure.

SIP entities MUST support the Dialog Event, RFC4235 [68].

3.1.1.2 REFER (transfer)

The REFER method MUST be supported within the ESInet/NGCS for two purposes:

- To transfer a call when the model is ad hoc, see Section 4.9 (transfer models)
- To conference additional parties to a call

REFER is defined in RFC 3515 [19]. The REFER method indicates that the recipient (identified by the Request-URI) should contact a third party using the contact information provided in the Refer-To header field of the request. The recipient of the REFER request sends an INVITE to the URI in the Refer-To header field.

REFER creates an implicit subscription as described in RFC 6665 [14] to a REFER event package. As with all SIP subscriptions the recipient of the REFER sends an immediate

© Copyright 2011-2022 National Emergency Number Association, Inc.

NOTIFY confirming instantiation of the subscription. When the INVITE is answered or fails, another NOTIFY is sent with success or failure of the REFER operation.

REFER is sometimes used with the Replaces header field, which is dubbed "REFER/Replaces". This is used to replace a call leg with another call leg, an example being replacing a two way call between the caller and call taker with a leg between the caller and the bridge, with another transaction used to create the leg between the call taker and the bridge. If an element receives a REFER with Replaces request when the Replaces SIP Call ID does not exist, it MUST be rejected.

If the calling device supports the Replaces header field, which is signaled by having the "replaces" value in the Supported header field of the original INVITE, the Replaces header field can be sent to the calling device in the context of an emergency call transfer when the model is ad hoc. Section 4.7 discusses the problem of a calling device that is unable to support a Replaces transaction. Section 4.7.2 discusses blind transfer which uses REFER without Replaces.

All SIP call processing entities within an NGCS, as well as PSAPs, MUST be able to send a REFER. Bridges MUST be able to receive a REFER. SIP entities implementing REFER MUST implement RFC 4508 [38] and the Replaces Header Field, RFC 3891 [27].

3.1.1.3 BYE (call termination)

The BYE method is used to terminate a call. BYE may be initiated from either end, unless the mechanism defined in Appendix C for implementing PSAP control of disconnect is used.

3.1.2 Methods allowed to be initiated by any UA which MUST be supported by i3 elements

3.1.2.1 CANCEL (cancel call initiation)

An attempt to create a call with INVITE MAY be cancelled before it is completed using the CANCEL method. CANCEL is used before the session is created (call establishment); BYE is used after the session is created. Of course, race conditions exist between the signaling of the session and the attempt to cancel it. These conditions are discussed in RFC 3261 [10]. CANCEL would be the signaling used to abandon a call, and NGCS elements MUST treat a CANCELled call as such, including logging requirements.

3.1.2.2 UPDATE (update parameters)

UPDATE is defined in RFC 3311 [15] and is sometimes used during call establishment if needed to change the parameters of the call. RFC 3311 states that although UPDATE can be used on confirmed dialogs, it is RECOMMENDED that a re-INVITE be used instead.

© Copyright 2011-2022 National Emergency Number Association, Inc.

NGCS elements MUST NOT send UPDATE on a confirmed dialog but MUST accept one. UPDATE MAY be used on any call within an ESInet/NGCS (including 9-1-1 calls).

3.1.2.3 OPTIONS (option negotiation)

OPTIONS MAY be used by an external caller, or inside the ESInet/NGCS to determine the capabilities of the destination User Agent (UA). All endpoints within the ESInet/NGCS MUST be capable of responding to an OPTIONS request, as defined in RFC 3261 [10].

Although Session Timers [32] MUST be supported by all SIP entities, an OPTIONS transaction is the preferred mechanism for maintaining a "keep alive" between two SIP elements. Periodic OPTIONS transactions MUST be used between ESRPs that normally pass calls between themselves, between the ESRP and the PSAPs, LNGs and LPGs it normally serves, and between the PSAP and the bridge it normally uses. The period between OPTIONS requests used for keep-alive SHOULD be provisioned, and default to one (1) minute (which MUST be less than the Transport Layer Security (TLS) timeout period) intervals during periods of inactivity. Since the OPTIONS method requires an exchange of messages, only one member of a pair of "adjacent" SIP elements needs to initiate an OPTIONS request towards the other. It is RECOMMENDED that the "upstream" element initiates the request. A Session Recording Client (SRC) sends OPTIONS requests to its Session Recording Service (SRS) for keep-alive purposes. Using an OPTIONS request from outside the ESInet/NGCS is NOT RECOMMENDED to determine if an emergency call would reach the PSAP. Instead, sparing use of the Test Call (RFC 6881) [46] mechanism is RECOMMENDED. If OPTIONS is received from an entity outside the ESInet/NGCS, it SHOULD receive a valid response from some entity inside the ESInet/NGCS. The ESRP SHOULD route the request to some entity that will respond affirmatively. The path taken by such a request need not be representative of what an actual or test call would take. The ESRP itself, if it had some UA capability, SHOULD respond.

3.1.2.4 ACK (acknowledgement)

The ACK request is used to acknowledge completion of a request. Strictly speaking, there are two cases of ACK: one used for a 2XX series response (which is actually part of a three-way handshake, typically INVITE/200 (OK)/ACK), and a non-2XX response, which is a separate transaction. All endpoints in an ESInet/NGCS MUST use ACK.

3.1.2.5 PRACK (reliable message acknowledgement)

The PRACK method MUST be used within systems that need reliable provisional responses (non 100). "Provisional" responses are part of the 1XX series responses, except the general 100 (Trying) response. As an example of when an NGCS SIP element may see a PRACK,

© Copyright 2011-2022 National Emergency Number Association, Inc.

see the example in RFC 3311 [15] when PRACK is sent by the UAS to reliably send an SDP "offer" to a UAC in a 18X response.

3.1.2.6 MESSAGE (text message)

The MESSAGE method, an extension to SIP, allows the transfer of Instant Messages and is also used to carry a Common Alerting Protocol (CAP) message. In NG9-1-1, Message Session Relay Protocol (MSRP) is used to carry Instant Messages, but the MESSAGE method is used for non-interactive calls. Since the MESSAGE request is an extension to SIP, it inherits all the request routing and security features of that protocol. MESSAGE requests carry the content in the form of Multipurpose Internet Mail Extensions (MIME) body parts. MESSAGE requests do not themselves initiate a SIP dialog; each Instant Message stands alone, much like pager messages. While there is no known use case, ESInet elements MUST allow MESSAGE requests in the context of a dialog initiated by some other SIP request. For more information on MESSAGE please refer to RFC 3428 [17]. MESSAGE is part of the SIP/SIMPLE presence and messaging system.

3.1.2.7 INFO

The INFO method (RFC 6086) [149] is used for communicating mid-session signaling information along the signaling path for a call. See Appendix C for details related to the use of INFO in the context of PSAP call control features. INFO MAY also be used for backwards compatibility with some video systems that use RFC 5168 [122] to request Intra-frame refresh (see Section 3.1.9.2). INFO MUST NOT be used to convey DTMF digits.

3.1.3 Methods used within the ESInet/NGCS

3.1.3.1 REGISTER

Use of REGISTER is not defined in this document, so REGISTER SHALL NOT be used.

3.1.3.2 SUBSCRIBE/NOTIFY (Events)

SUBSCRIBE/NOTIFY is a mechanism to implement asynchronous events notification between two elements. The mechanism is used in i3, for example, to request current state and updates to state from a remote element, and to obtain location from a SIP location reference. SUBSCRIBE requests SHOULD contain an "Expires" header field. This "Expires" value indicates the duration of the subscription. In order to keep subscriptions effective beyond the duration communicated in the "Expires" header field, subscribers MUST refresh subscriptions on a periodic basis using a new SUBSCRIBE message on the same dialog. The subscription also expires in the originating network when the associated SIP dialogue is terminated with a BYE.

© Copyright 2011-2022 National Emergency Number Association, Inc.

NOTIFY messages are sent to inform subscribers of changes (e.g., in state or location) to which the subscriber has a subscription. Subscriptions are typically put in place using the SUBSCRIBE method; however, it is possible for other means to be used. A NOTIFY message does not terminate its corresponding subscription. A single SUBSCRIBE request MAY trigger multiple NOTIFY requests.

For further information, refer to RFC 6665 [14] section 8.1. Entities implementing a notifier MUST implement RFC 3857 [26].

3.1.3.3 PUBLISH (update of presence information to presence server)

Use of PUBLISH is not defined in this document.

3.1.4 Response Codes

Responses typically encountered in a SIP call SHOULD be handled as follows:

(Only salient response codes are listed. Response codes not listed and not defined in RFC 3261 [10] are not expected to be provided nor received by the NGCS but if present, MAY be treated as the equivalent X00 error code, or MAY be processed as defined in the corresponding RFC.)

SIP Response Codes from NGCS	Description
180 (Ringing)	A 9-1-1 call is queued for answer. It is RECOMMENDED that no other 1XX response be used due to uneven implementations of these responses. 180 Ringing should be repeated at approximately 3-second intervals if the call is not answered.
200 (OK)	Normal response to an answered call.
3XX	9-1-1 calls are usually not redirected, and thus 3XX responses are normally not used. 3XX MAY be used for calls within the ESInet. NG9-1-1 elements that initiate calls within the ESInet SHOULD appropriately respond as defined in RFC 3261 [10].
400 (Bad Request)	A 9-1-1 call is so malformed that the BCF cannot parse the message.
401 (Unauthorized)	MUST NOT occur for a 9-1-1 call.
402 (Payment Required)	SHOULD NOT occur for a 9-1-1 call or an internal call.

© Copyright 2011-2022 National Emergency Number Association, Inc.

SIP Response Codes from NGCS	Description
403 (Forbidden)	Normally, 403 (Forbidden) SHOULD NOT occur, but if the BCF passes a malformed INVITE which downstream devices cannot handle, they may have no choice but to return 403.
404 (Not Found)	404 (Not Found) would normally not occur for a 9-1-1 call, but MAY be used within the ESInet.
406 (Not Acceptable)	The 406 (Not Acceptable) SHOULD NOT occur for a 9-1-1 call because the INVITE SHOULD NOT have an Accept header field that is unacceptable to the PSAP. If it does, 406 is the correct response.
407 (Proxy Authorization)	Proxy authorization is REQUIRED for all calls originated by entities within an ESInet/NGCS.
408 (Request Timeout)	MAY be issued in an unplanned circumstance. Normally, this SHOULD NOT happen to a 9-1-1 call.
413 (Request Entity too Large)	The BCF SHOULD accept any Request-URI, but downstream elements MAY return 413 (Request Entity Too Large).
414 (Request-URI Too Long)	The BCF SHOULD accept any Request-URI, but downstream elements MAY return 414 (Request-URI Too Long).
416 (Unsupported URI Scheme)	The BCF SHOULD accept any Request-URI, but downstream elements MAY return 416 (Unsupported URI Scheme).
486 (Busy Here)	PSAPs MAY limit the number of test calls, and if that limit is exceeded, the response SHALL be 486 Busy Here. 486 may also be generated by a race condition in the queue mechanism overload per section 4.2.1.3
500 (SIP Server Internal Error)	Indicates a failure in a system, or a failure to be able to process the call. Depending on the source of the failure, retry may succeed.
600 (Busy Everywhere)	If the BCF detects an active attack, it MAY respond with 600 (Busy Everywhere), rather than another 4XX response, although silent discard may be more effective. It is also returned by the Busy Policy Routing Rule "busy action"

© Copyright 2011-2022 National Emergency Number Association, Inc.

3.1.5 Header fields and Request URI supported at the interface to the NGCS

The Best Current Practice for Communications Services in Support of Emergency Calling RFC 6881 [46] document referenced in this section contains normative text related to devices, originating network, and service providers. This document considers only the interface between an originating network and the NGCS with respect to the signaling of the emergency calls and callbacks between an OSP and the NGCS. References to RFC 6881 in this document are limited to requirement ED-62, the details of signaling for an emergency call. Accordingly, it shall be explicitly understood that all requirements referenced from RFC 6881, regardless of wording and context in that document, SHALL apply only to the NGCS interface and SHALL NOT constrain or limit the signaling and procedures used by end devices, access networks, and originating networks when not interacting with the NGCS. The following table shows the SIP header fields required in the INVITE and MESSAGE methods for emergency calls, recalling that the Request-URI will contain "urn:service:sos" or a subservice of it as defined in RFC 6881 [46] Section 5.

Only salient Header Fields are listed. Header Fields not listed and not defined in RFC 3261 [10] are not expected to be provided nor received by the NGCS but if present, MAY be ignored, or MAY be processed as defined in the corresponding RFC.

Header Field/Request	Defined In	See Section (or RFC 6881)	Notes
Identity	RFC 8224	[60]	Provides caller identity assertion using a cryptographically signed Personal Assertion Token (PASSporT) and associated parameters as defined in RFC 8225 [203]. Present on any call, added by STI-AS for outgoing calls.
Request-URI	RFC 3261 Section 8.1.1.1	ED62 1.	"urn:service:sos" or a subservice of it
To	RFC 3261 Section 8.1.1.2 & 20.39	ED62 2.	Usually sip:911 or "urn:service:sos" on an incoming call
From	RFC 3261 Section 8.1.1.3 & 20.20	ED62 3.	Content cannot be trusted unless protected by an Identity header field

© Copyright 2011-2022 National Emergency Number Association, Inc.

Header Field/Request	Defined In	See Section (or RFC 6881)	Notes
Via	RFC 3261 Section 8.1.1.7 & 20.42		Occurs multiple times, once for each SIP element in the path
CSeq	RFC 3261 Section 8.1.1.5 & 20.16		Defines the order of transactions in a session
Call-ID	RFC 3261 Section 8.1.1.4 & 20.8		This is the SIP call id, not the NG9-1-1 call id (e.g., "1j9FpLxk3uxtm8tn@biloxi.example.com" not "urn:emergency:uid:callid:1j9FpLxk3uxtm8"
Call-Info	RFC 3261 Section 8.1.1.10 & 20.9		Contains Additional Data URIs, Call and Incident Tracking IDs and EIDO URIs
Contact	RFC 3261 Section 8.1.1.8 & 20.10	ED62 5.	Usually a "globally routable user agent URI" (gruu) (RFC 5627) [41]
Content-Length	RFC 3261 Section 20.14		
Content-Type	RFC 3261 Section 8.2.3 & 20.15		Used, for example, in RFC 4119 [6] and RFC 4566[6] [12]
Geolocation	RFC 6442	ED62 8.	Only occurs in an emergency call
Geolocation-Routing	RFC 6442	ED62 8.	Specifies if the Geolocation header field can be used for routing. Only occurs in an emergency call

[6] Examples may include application/pidf+xml to indicate a PIDF-LO in the body of the message and application/sdp to indicate use of Session Description Protocol (SDP) in the body of the message.

© Copyright 2011-2022 National Emergency Number Association, Inc.

Header Field/Request	Defined In	See Section (or RFC 6881)	Notes
History-Info	RFC 7044		MAY indicate the call has been retargeted, MUST include a Reason header field per section 3.1.8
P-Access-Network-Info	RFC 3325		MAY contain cell site info in carrier specific formats in an incoming call
P-Asserted-Identity	RFC 3325		When present, typically overrides the From header field
P-Preferred-Identity	RFC 3325	3.1.15, 6.1.2.2	Used with unauthenticated (e.g., NSI) calls
Reason	RFC 3326		Included if an INVITE transaction is retargeted.
Route	RFC 3261 Section 20.34	ED62 4.	Usually the ESRP/PSAP URI on an incoming emergency call
Supported	RFC 3261 Section 8.1.1.9 & 20.37	ED62 7.	
Replaces	RFC 3891	4.7	Used in call transfer scenarios

3.1.6 Header fields Accepted and also used internally

Only salient Header Fields are listed. Header Fields not listed and not defined in RFC 3261 [10] are not expected to be provided nor received by the NGCS but if present, MAY be ignored, or MAY be processed as defined in the corresponding RFC.

Header Field	Defined In	Notes
Max-Forwards	RFC 3261 20.22	Specifies the maximum number of SIP elements that may be traversed before assuming a routing loop has occurred
Accept-Contact	RFC 3841	
Accept	RFC 3261 20.1	
Content-Encoding	RFC 3261 20.12	
Accept-Encoding	RFC 3261 20.2	

© Copyright 2011-2022 National Emergency Number Association, Inc.

Header Field	Defined In	Notes
Content-Language	RFC 3261 20.13	
Accept-Language	RFC 3261 20.3	
Content-Disposition	RFC 3261 20.11	
Record-Route	RFC 3261 20.30	
Allow	RFC 3261 20.5	
Unsupported	RFC 3261 20.40	
Require	RFC 3261 20.32	
Proxy-Require	RFC 3261 20.29	
Expires	RFC 3261 20.19	
Min-Expires	RFC 3261 20.23	
Subject	RFC 3261 20.36	
Priority	RFC 3261 20.26	
Date	RFC 3261 20.17	
Timestamp	RFC 3261 20.38	
Organization	RFC 3261 20.25	
User-Agent	RFC 3261 20.41	
Server	RFC 3261 20.35	
Authorization	RFC 3261 20.7	
Authentication-Info	RFC 3261 20.6	
Proxy-Authenticate	RFC 3261 20.27	
Proxy-Authorization	RFC 3261 20.28	
WWW-Authenticate	RFC 3261 20.44	
Warning	RFC 3261 20.43	
Error-Info	RFC 3261 20.18	
Alert-Info	RFC 3261 20.4	
In-Reply-To	RFC 3261 20.21	
MIME-Version	RFC 3261 20.24	
Reply-To	RFC 3261 20.31	
Retry-After	RFC 3261 20.33	
RAck	RFC 3262 7.2	
RSeq	RFC 3262 7.1	
Event	RFC 6665 8.2.1	
Allow Events	RFC 6665 8.2.2	
Subscription-State	RFC 6665 8.2.3	

© Copyright 2011-2022 National Emergency Number Association, Inc.

Header Field	Defined In	Notes
Resource-Priority	RFC 4412 3.1, Section 3.1.7	

3.1.7 Resource Prioritization

The Resource-Priority header field (RFC 4412 [37]) is used on SIP calls to indicate priority that proxy servers give to specific calls. All SIP user agents that place calls within the ESInet/NGCS MUST be able to set Resource-Priority. All SIP proxy servers in the ESInet/NGCS MUST implement Resource-Priority and process calls in priority order when a queue of calls is waiting for service at the proxy server and, when needed, preempt lower priority calls[7]. BCFs[8] MUST police Resource-Priority of incoming SIP calls when the value comes from the "esnet" namespace. Any other namespace is ignored. BCFs MUST add a Resource-Priority header with an appropriate value from the "esnet" namespace if it is not present and should be included. BCFs MUST change or delete a value that is present on an incoming call that appears to be invalid or illegitimate. Those calls that appear to be emergency calls (such as those To: 911 but without a Request-URI of "urn:service:sos") MUST be marked with a provisioned Resource-Priority, which defaults to "esnet.1". PSAP callbacks during handling of an incident use "esnet.0". Callbacks outside of an incident are not marked. ESInets normally use the "esnet" namespace.

The use of the namespace in an ESInet is defined as:

Header	Description
esnet.0	Calls which relate to an incident in progress, but whose purpose is not critical
esnet.1	9-1-1 calls traversing the ESInet
esnet.2	Calls related to an incident in progress which are deemed critical
esnet.3-esnet.4	not defined

[7] Mechanisms such as DiffServ are likely to be sufficient to assure that high priority traffic gets through an ESInet. Preemption is unlikely to be needed, even for very high priority responder traffic, and should not be used for 9-1-1 calls. However, if responders need resources, lower priority traffic may have to be cleared to provide such resources. Preemption is considered a necessary prerequisite to getting police and fire responders on an ESInet. Originating network operators have expressed concerns over preemption especially for 9-1-1 calls.

[8] This function may be provided outside an SBC but within the BCF.

© Copyright 2011-2022 National Emergency Number Association, Inc.

3.1.8 History-Info and Reason Parameter

When a call is not sent to the originally intended destination, for example when it is diverted by the ESRP to another PSAP, the final destination must have the ability to know why it got the call. For this reason, SIP elements in the NGCS MUST support the History-Info header field (RFC 7044 [35]) and a Reason header field. Elements that retarget a call MUST add a History-Info header field indicating the original intended recipient, and the reason why the call was retargeted. A 'text' parameter MUST also be supplied to further explain why the call was retargeted. NGCS elements MUST be prepared to handle a History-Info (and its associated Reason parameter) added by an element outside the ESInet before presentment to the 9-1-1 system. History-Info might be found in a call in other circumstances, such as a RouteAction with a cause code of "Normal-Next-Hop", code 200. This document defines a new "Reason Protocol" to be used with the Reason header field for emergency call retargeting not due to normal SIP protocol mechanisms. The protocol value is 'emergency'. A registry is defined for cause codes (See Section 10.20) used for the SOS protocol value. The initial values of 1-10 are used for Policy Routing Rule (PRR) retargeting. The first time the ruleset is evaluated, the cause code SHALL be set to 1. Every time the rule set is re-evaluated for the same call (such as when the targeted PSAP refuses the call), the cause code is incremented by one. When cause codes 1-10 are used, the 'text' parameter MUST be present, and must start with the ruleId followed by a colon and any other clarifying text the implementation wishes to add.

3.1.9 Media

All call handling elements MUST support media using Real-time Protocol (RTP) (RFC 3550 [11]). Each SIP session initiation message or response SHOULD describe the media the User Agent is capable of supporting using Session Description Protocol (SDP) (RFC 4566 [12]) in the body of the message. Support of any type of media (e.g., voice, video, text) in originating networks is based on regulatory requirements or business decisions. All elements in the ESInet/NGCS MUST support all media if offered, except that a legacy PSAP on a Legacy PSAP Gateway MAY only support audio, including Teletypewriter (TTY) tones when converted from Real Time Text (RTT).

Media streams for voice, video, and text MUST be carried on RTP over UDP (User Datagram Protocol). All endpoints in an ESInet MUST implement media security with Secure Real Time Protocol (SRTP) using Datagram Transport Layer Security (DTLS) as specified in RFC 5763 [166] and RFC 5764 [167]. SRTP Security MUST be requested in all calls originated within an ESInet. If a call is presented to the ESInet with SRTP, SRTP

© Copyright 2011-2022 National Emergency Number Association, Inc.

MUST be maintained through the ESInet[9]. Since media are routinely logged, the Logging Service MUST maintain equivalent or better security on the logging (recording) session as that provided on the emergency call (communications) session. RTCP as defined in RFC 3550 [11] and Secure Real Time Control Protocol (SRTCP) as defined in RFC 5764 [167] MUST be supported within the ESInet, and it is highly RECOMMENDED that all calls presented to the ESInet provide RTCP. Within the ESInet, all User Agents MUST support RTCP Extended Reports (RTCP XR) [65]. SIP User Agents within the ESInet SHOULD label all media

Instant Messaging (IM) MUST be presented to the ESInet/NGCS using Message Session Relay Protocol (MSRP) [91] as the media stream.

All elements in the ESInet/NGCS MUST support RFC 5888 [20], RFC 3605 [22], RFC 3581 [21] and RFC 4574 [99]

3.1.9.1 Audio

To minimize transcoding requirements, it is desirable that User Agents in the ESInet/NGCS and in i3-PSAPs implement the maximum number of codecs used in the market.

All User Agents in the ESInet/NGCS MUST support G.711 μ-law and A-law codecs. A-law support is REQUIRED in those cases in which devices manufactured primarily for non-North American markets are used within North America.

The following table lists widely used audio codecs, whether they are available under license and their support requirements.

Name	Definition and Usage	Licensed	Support
G.711μ-law	Narrowband audio. Widely used by Voice over IP (VoIP) devices manufactured for North America and Japan. Supports North American DTMF tones inband.	No (free)	REQUIRED
G.711 A-law	Narrowband audio.	No (free)	REQUIRED

[9] Some PSAPs may be subject to the Health Insurance Portability and Accountability Act (HIPAA), or a state equivalent. Maintaining privacy via SRTP MAY be required on all calls for such PSAPs, and media handling systems on the ESInets MAY need to support such capability by applying SRTP to those media regardless of whether SRTP was applied to the call when presented.

© Copyright 2011-2022 National Emergency Number Association, Inc.

Name	Definition and Usage	Licensed	Support
	Widely used by VoIP devices manufactured for Europe and Asia. **Note**: DTMF tones are different in Europe & Asia; no support in the North American Market.		
EVS (Enhanced Voice Service)	Audio codec supporting Narrowband, Fullband, Wideband and Superwideband.	Yes	RECOMMENDED
AMR (a.k.a. AMR-NB)	Common Narrowband audio. Used in CDMA, GSM, 3G, LTE networks	Yes	RECOMMENDED
AMR-WB (G.722.2)	Common Wideband audio (HD Voice). Used in CDMA, GSM, 3G, LTE networks	Yes	RECOMMENDED
G.722	High Definition Voice (HD Voice). Wideband (high compression, high quality voice).	No (free)	RECOMMENDED
G.729AB	Wideband audio codec Used in VoIP networks.	Yes	OPTIONAL
OPUS	Open Source codec (RFC 6716 [212]). Being implemented by major providers.	No (free)	RECOMMENDED

3.1.9.2 Video

All User Agents in the ESInet/NGCS MUST support video compression format H.264/MPEG-4 Version 10. The Baseline profile MUST be supported. Scalable baseline profile support is RECOMMENDED. At least levels 1-3 MUST be supported. User Agents in the ESInet/NGCS MUST support both RFC 5104 [121] and RFC 5168 [122] for full frame refresh requests. The RFC 5104 Real-time Control Protocol (RTCP) method is preferred with fall back to RFC 5168 INFO method when the sender does not implement RFC 5104. To maintain the ability to support rapid finger-spelling for sign language users, ESInet/NGCS elements must attempt to maintain 30 frames per second video if offered by the sender. RTP/AVPF (RFC 4585 [123]) MUST be supported and is preferred in offers.

© Copyright 2011-2022 National Emergency Number Association, Inc.

3.1.9.3 Real-Time Text

All call handling elements in the ESInet/NGCS MUST support RTP Payload for Text Conversation (RFC 4103) [85]. All except the LNG and LPG MUST also support the update for multi-party real-time text calls defined in *RTP-Mixer Formatting of Multiparty Real-Time Text* (RFC 9071) [219]. Information on application of real-time text can be found in Framework for Real-Time Text over IP Using the Session Initiation Protocol (SIP) (RFC 5194 [84]).

3.1.9.4 TTY (Baudot tones)

NG9-1-1 anticipates that deaf and hard of hearing callers will migrate from TTY to other forms of communication including Real-Time Text devices and various forms of relay. Although use of TTY is expected to decline, it cannot be assumed that TTY will be completely gone by the time transition to NG9-1-1 is complete. Therefore, PSAPs MUST be capable of receiving calls from TTY devices.

Handling Baudot tones within an IP (VoIP) network is very problematic. Baudot is much more sensitive to packet loss and other impairments than human voice. Transcoding from Baudot to RFC 4103 [85] Real-Time Text is usually the only practical way to send TTY messages across an IP network. If at all practical, transcoding SHOULD occur in the originating network as close to the TTY device as possible. However, it is very difficult to assure that all originating networks will do that transcoding. Therefore, ESInets/NGCS must have the ability to transcode. LNGs and LSRGs MUST transcode, and therefore it is the VoIP originating networks that are problematic in that they may present calls containing Baudot tones to the ESInet/NGCS. A transcoder MUST be placed as early in the media path as possible[10], and the IP network between the originating network and the transcoder MUST be engineered to have very low packet loss and minimize other impairments. The transcoder MUST be compliant with RFC 5369 [86] and MUST be transparent to audio that is not Baudot tones. Transcoders SHOULD reduce the amplitude of detected Baudot tones but SHOULD NOT remove them entirely. PSAPs that receive calls from sources other than the ESInet/NGCS may need to handle TTY in another way, which is outside the scope of this document.

[10] It would be desirable for the transcoder to be part of the BCF, but this may not be possible. If it is not part of the BCF it would be internal to the ESInet and the engineering of that part of the ESInet must assure that there is very low packet loss or other impairments.

© Copyright 2011-2022 National Emergency Number Association, Inc.

3.1.10 Instant Messaging

Text-based communications for NG9-1-1 is supported by all call handling elements of an NG9-1-1 system in two ways: Real-Time Text (RTT) and Instant Messages (IM)[11], with location and the ability to support location updates.

All call handling elements MUST support Message Session Relay Protocol (MSRP), RFC 4975 [88], chat rooms, RFC 7701 [123], as well as RFC 4976 [89] and RFC 3994 [87]

Location MUST be included in a Geolocation header field in the initiation of the MSRP session as with any other "call" to 9-1-1.

Other Instant Messaging protocols such as XMPP MAY be supported by an originating network but MUST be interworked to MSRP prior to presentation to the ESInet/NGCS.

3.1.11 Non-interactive calls

Non-interactive calls, also called data-only emergency calls, are emergency calls that are initiated automatically, carry data, are not necessarily associated with a person, and do not establish two-way interactive media sessions.

Non-interactive calls[12] presented to an ESInet are signaled with a SIP MESSAGE method containing a Common Alerting Protocol (CAP) [66] message (as described in RFC 8876 [225]), possibly wrapped in an Emergency Data eXchange Language – Distribution Element (EDXL-DE) [78] wrapper. The <Area> element of the CAP message is copied, in PIDF-LO form, in a Geolocation header field of the SIP MESSAGE container. The CAP message is included in the body of the SIP MESSAGE, with a MIME type of application/common-alerting-protocol+xml.

The MESSAGE MUST conform to section 3.1.15 with respect to Additional Data.

The <Identifier> in the CAP message is not the same as the Call Identifier assigned in the ESInet/NGCS, but the log contains a record that correlates the two.

The <Sender> SHOULD be the same as the From header field in the MESSAGE.

---

[11] All ESInet elements support instant messaging using the specifications in this document. Any given originating network or device may not support instant messaging, and support of instant messaging by originating networks and devices may be subject to regulation.

[12] All ESInet elements support non-interactive calls using the specifications in this document. Any given originating network or device may not support non-interactive calls, and support of non-interactive calls by originating networks and devices may be subject to regulation.

© Copyright 2011-2022 National Emergency Number Association, Inc.

If included, the <Addresses> element SHOULD contain "urn:service:sos", the same as the Route header field for the Message.

Automatic Crash Notification (AACN) calls (see Section 3.1.19) establish interactive media and are associated with human vehicle occupant(s), instead of non-interactive calls (which do neither). A non-interactive call from a vehicle might be placed by an element that is not designed to communicate with vehicle occupants (e.g., a sensor module embedded in the vehicle without speaker or microphone access) and does not provide interactive two-way media.

If an <Area> element is included, at least one <Polygon> or <Circle> element MUST be included. Any <AreaDesc> and <Geocode> elements will not be used by the routing elements, although destination agencies may be able to make use of them. The Geolocation header field in the MESSAGE MUST have the PIDF-LO equivalent of the <Polygon> or <Circle> element(s).

A digital signature SHOULD be included in the CAP message. The CAP message SHOULD NOT be encrypted.

When the CAP message is enclosed in an EDXL-DE wrapper, the body of the SIP MESSAGE will contain a section application/emergency-data-exchange-language+xml.

Non-interactive calls are routed and handled the same as voice, video, or text calls throughout the NG9-1-1 system. The routing mechanisms can route non-interactive calls differently from voice calls in the same way they can route video calls differently from voice calls. The parameters in the CAP message are available to the Policy Routing Function (PRF) as inputs to direct calls with specified characteristics to specific entities.

3.1.12 Bodies in messages

All SIP elements in an ESInet/NGCS MUST support multipart MIME as defined in RFC 2046 [90]. For example, location, Additional Data blocks (RFC 7852) [107], and SDP may be present in a message body. All SIP elements in the NGCS MUST allow all mime types/body parts to pass to the PSAP.

3.1.13 Transport

All SIP elements MUST support TLS (See Section 2.8.1), TCP, and UDP transport. SIP signaling within the ESInet SHOULD be carried with TLS. If TLS transport fails or is not available, SIP elements SHOULD attempt to use TCP. If TLS and TCP transports both fail or are unavailable, SIP elements SHOULD fall back to UDP transport. It should be noted however that emergency call-related SIP messages have many large elements (for example, a PIDF-LO) and are more likely to be fragmented at the source when carried in

© Copyright 2011-2022 National Emergency Number Association, Inc.

UDP[13]. Packet fragmentation and defragmentation is fully supported in IPv4 however, in-transit fragmentation is not supported in IPv6. To avoid packets being dropped in transit because of size, IPv6 Path Maximum Transmission Unit Discovery (PMTUD) [234] MAY be used. It should be noted however that PMTUD utilizes Internet Control Message Protocol for IPv6 (ICMPv6) [235] to convey error responses back. Unfortunately, ICMP traffic is often blocked by firewalls in IP networks, which means the error response is never reaching the sender thus causing the packet to be lost and the sender not knowing that it has to reduce path MTU for the next packets it sends. Perfect Forward Security MUST be implemented and all SIP elements within the NGCS MUST support connection reuse, RFC 5923 [217].

Further, if the transport is not TLS, additional security weaknesses occur, and implementations MUST be prepared to deal with the security risks engendered when TLS protection is not available. Known attacks on incomplete fragmentation/reassembly implementations are another concern that MUST be addressed by all elements in the ESInet. Persistent TLS connections between elements that frequently exchange SIP transactions SHOULD be deployed.

PSAPs are expected to detect the presence of RTP streams so they can distinguish RTP failure from real silence by the caller. Devices containing User Agents that are not part of a Back-to-Back User Agent (B2BUA) and that detect the loss of RTP SHOULD attempt to re-establish the streams by sending a re-INVITE to the other party. If that fails, the device SHOULD indicate a failure and provide a mechanism for taking action such as initiating disconnect. A call SHOULD NOT automatically be taken down if RTP streams fail. For example, a multimedia call which loses one of several streams SHOULD NOT be terminated, just for loss of some media.

3.1.14 Call Routing

All SIP elements MUST support routing of SIP messages per RFC 3261 [10] and RFC 3263 [13]. Note particularly that URIs will often have the domain of the destination following the '@' rather than the hostname of a SIP server, and thus DNS SRV records (RFC 2782) [75] MUST be consulted to determine the hostname of the SIP server for that domain. Redundancy support for a SIP call MUST NOT depend on non-standard mechanisms in SIP elements. Only mechanisms such as UPDATE or re-INVITE with a modified Contact and out-of-dialog REFER, which only rely on aspects of standards this document requires of all

[13] Note that the typical length of a SIP INVITE is around 1300 bytes including around 200 bytes for the SIP Header overhead. If, for example, a SIP INVITE contains a complete header, and a body containing both an SDP and a civic PIDF-LO, it is likely this SIP message may be too big for a single UDP packet; and may require fragmentation, which is sometimes problematic. TCP transport avoids such issues.

© Copyright 2011-2022 National Emergency Number Association, Inc.

SIP elements in the ESInet, MUST be used to perform re-home on an established SIP dialog in the case of host failure.

Emergency call handling relies on the Service URN in the Request-URI being preserved. To avoid the Request-URI being rewritten, this document assumes loose routing (as defined in RFC 3261 [10]) is used for all SIP Calls end-to-end. Per RFC 3261, the "lr" parameter should be present in URIs used for routing. A future version of this document will normatively require this behavior.

3.1.15 Originating Network Interface

The originating call interface to the ESInet/NGCS is a SIP call interface as described above in Section 3.1. All calls MUST be routed the same way they would route if the location in the call was used to query the authoritative ECRF. Location MUST be included in the Geolocation header field (civic or geodetic) by reference or value. The location used to query the routing function MUST be included in the Geolocation header field of the outgoing INVITE or MESSAGE method. The call MUST be routed, using normal RFC 3261 [10] procedures, to the URI obtained from the routing function using the "urn:service:sos" service URN (this URI should contain the "lr" parameter in the SIP INVITE to avoid Request-URI rewriting). A callback address MUST be included in the outgoing INVITE or MESSAGE method, with an immediate device callback in the Contact header field and an address of record for later callback in either the From header field (protected by the Identity header field) or a P-Asserted-Identity (P-A-I).

A call from an unauthenticated device SHALL populate the P-Preferred-Identity header field in the INVITE request with an equipment identifier as a SIP URI and no P-Asserted-Identity SHALL be provided.

The incoming INVITE or MESSAGE method to the ESInet/NGCS MUST include Call-Info header field values containing URIs that refer to Additional Data (RFC 7852) [107] "ProviderInfo" and "ServiceInfo" structures. This is indicated by "purpose" parameters of "purpose=EmergencyCallData.ProviderInfo" and "purpose=EmergencyCallData.ServiceInfo" (respectively). Additional Call-Info header field values MAY be included that contain a URI(s) that refers to other Additional Data blocks. Some providers MAY also include a "SubscriberInfo" block.

Elements on an ESInet SHALL assume a SIP call entering the ESInet is an emergency call unless it can determine it is something else, such as a call to an administrative number. Even if the call does not have the emergency service URN in the Request-URI, the call SHOULD be assumed to be an emergency call and the Request-URI SHALL be rewritten to urn:service:sos by the BCF or originating ESRP.

© Copyright 2011-2022 National Emergency Number Association, Inc.

3.1.16 PSAP Interface

The PSAP call interface is a SIP call interface as described in Section 3.1. All calls will be presented to the PSAP based on the terminating ESRP's Policy Routing Function (PRF), defined in Section 4.2.1.5. The Geolocation header field, Call-Info header fields and other header fields SHOULD be the same as above (Section 3.1.15). The call will be routed, using normal RFC 3261 [10] procedures, to the URI obtained from the ESRP's PRF. See Section 4.6.1 for other information on the PSAP interface.

3.1.17 Element Overload

Any SIP element may encounter a condition in which it is asked to process more calls than it can handle. SIP element overload has been extensively studied (see RFC 6357 [81]). Simple mechanisms to handle overload are insufficient. This standard specifies methods to avoid overload of calls to specific agencies using the routing rule and queue mechanisms, but a given SIP element may still encounter overload. To cope with such overload, all SIP elements MUST implement the overload control mechanisms described in RFC 7339 [56].

3.1.18 Maintaining Connections and NAT Traversal

All elements in an ESInet that implement SIP interfaces MUST comply with RFC 5626 [42] (Outbound) to maintain connections from User Agents. PSAPs, IMRs, bridges and other elements that terminate calls from entities outside an ESInet that may be behind NATs MUST implement "Interactive Connectivity Establishment (ICE)", RFC 8445 [44] which includes support for "Session Traversal Utilities for NAT (STUN), RFC 5389 [83]. ESInets/NGCS SHOULD maintain a "Traversal Using Relays around NAT (TURN)" (RFC 5766) [119] server for use by entities inside the ESInet placing outbound calls.

3.1.19 Advanced Automatic Crash Notification Calls

Advanced Automatic Crash Notification (AACN) calls, also called telematics calls, are emergency calls placed by vehicles or (Telematic Service Providers) (TSPs), initiated either automatically or manually, establishing interactive media channels, and conveying telematics data. The term "automatic crash notification" is used even though such calls are not necessarily in response to a crash and may be initiated manually as well as automatically; the telematics data they carry is often called "crash data" even though a crash has not necessarily occurred. In some older documents the word "collision" is used instead of "crash". The term Next Generation-Advanced Automatic Notification Calls (NG-AACN) is used to refer to AACN calls which conform to this document and the relevant IETF standards.

Depending on implementation, the originator of an AACN call might be a vehicle or TSP on behalf of a vehicle. Communication between the vehicle and TSP is out of scope, but it is

© Copyright 2011-2022 National Emergency Number Association, Inc.

assumed that the TSP relays or passes information between the vehicle and PSAP (e.g., requests for updated data or for the vehicle to perform an action such as flashing lights, providing access to a camera, unlocking doors, etc.).

NG-AACN calls are specified in RFC 8148 [168]. As described there, vehicles (or TSPs) attach a Vehicular Emergency Data Set (VEDS) telematics dataset as described in VEDS, Version 3 [169] and a metadata/control object (RFC 8148) [168] containing vehicle/TSP capabilities information, to the SIP INVITE message that initiates an AACN call; the PSAP attaches a metadata/control object containing an acknowledgment that the dataset was received to its final response to the INVITE. When the vehicle (or TSP) receives the acknowledgement, it indicates not only that the PSAP received the VEDS data, but also that the call is a NG-AACN call end-to-end. If the vehicle (or TSP) receives the final response to an INVITE that lacks an acknowledgement of the VEDS data, this indicates that the call is not NG-AACN end-to-end (e.g., the call is being handled by a legacy PSAP or there is a legacy gateway at some point in the call path); the vehicle/TSP then falls back to legacy means of conveying crash and location data (e.g., text-to-speech, prerecorded audio, or verbal interaction with the TSP assistant).

i3 PSAPs MUST support NG-AACN calls per RFC 8148 [168], including at least the VEDS dataset and the ability to send a telematics dataset acknowledgment. A PSAP MAY support additional telematics datasets (e.g., a PSAP might support the Pan-European eCall Minimum Set of Data (MSD) as described in RFC 8147 [202] to be prepared in case a vehicle sends the wrong dataset for North America), and MAY support enhanced capabilities of NG-AACN calls as described in RFC 8148 [168], (e.g., the ability to request a vehicle/TSP to send an updated or different dataset or to take some other action, such as flashing the lights, unlocking the doors, or accessing a vehicle camera feed).

The VEDS dataset was created by a Joint Association of Public-Safety Communications Officials (APCO)/NENA working group to carry telematics data useful in handling emergency calls. Per RFC 8148 [168], the data is normally carried by value in the initial SIP INVITE message and therefore can be presented to the call taker when a call is assigned. An i3 PSAP MAY request a new VEDS dataset at any time during the call (e.g., if a call taker wants to check if the vehicle's condition, number of occupants, or location has changed). The vehicle/TSP MAY send an updated unsolicited VEDS dataset during the call as described in RFC 8148 [168] (e.g., if it is aware that data previously sent has changed).

The VEDS dataset contains a comprehensive set of fields. It does not specify which fields vehicles must populate. Vehicle manufacturers and telematics vendors/providers are encouraged to populate as many fields as possible. The most critical fields are currently considered to be:

- Vehicle VIN, year, make, model

© Copyright 2011-2022 National Emergency Number Association, Inc.

- Impact velocity
- Vehicle location
- Air bag deployment (i.e., indicating which airbags deployed)
- Vehicle final resting orientation (e.g., on driver's side, on roof)
- Number of occupants
- Seat belt status
- Hazardous cargo indicator(s)
- Timestamp
- Recent previous location
- Call back number (e.g., to driver cellphone or vehicle cell number)

The call taker may request the vehicle to perform an action (e.g., flashing lights, unlocking doors, view the feed from a vehicle camera). Such requests and responses are normally done during a call by using the SIP INFO method, as described in RFC 8148 [168]. It is OPTIONAL for vehicles and PSAPs to support actions (other than sending an updated dataset). It is RECOMMENDED that vehicles and PSAPs support such actions.

The call routing mechanism defined in this document can route NG-AACN calls specially if desired (e.g., cooperating PSAPs might choose to have all NG-AACN calls handled by a designated PSAP). The parameters in the initial INVITE message that indicate that the call is an NG-AACN call are available to the Policy Routing Function [3.3] (e.g., the Request-URI, a Call-Info header field with a "purpose" parameter value of "EmergencyCallData.VEDS", and a MIME body part of "Application/EmergencyCallData.VEDS" each indicate an AACN call).

3.2 Location

Location is fundamental to the operation of the 9-1-1 system. Location is provided outside the ESInet/NGCS, and the generic functional entity that provides location is a Location Information Server (LIS). Since the LIS is external to the NGCS, the LIS is out of scope for i3. However, the entities inside the ESInet MUST interact with a source of location and thus the interfaces to that function are in scope and defined herein. For the purposes of this document, the only capabilities a LIS provides that are relevant to i3 are:

a) A de-reference function defined below for location by reference
b) Validation of location stored in the LIS by performing a validation query against the i3 LVF using the civic addresses, as described in Section 3.4.2.

Any element that provides either or both of these two capabilities is considered a LIS within i3. Although a LIS is defined as a "server", as with all elements defined in this document, there may not be a physical server, and indeed, a LIS for some networks may only be a protocol interwork function to some other element in the network.

© Copyright 2011-2022 National Emergency Number Association, Inc.

The NG9-1-1 system supports location included by value in the body of a SIP message, with a pointer to it (i.e., a cid URL) in the Geolocation header field (RFC 6442) [8] of the SIP message. It also supports location by reference, when a location URI is populated in the Geolocation header field. All NGCS that receive location as a PIDF-LO must be prepared to receive location by reference and to use location by reference the NGCS MUST implement SIP and HTTP Enabled Location Delivery (HELD) (RFC 5985) [7] de-referencing protocols. A Location Information Server (LIS)[14] MUST implement one or both of these protocols.

Location by reference using SIP is an implied subscription to Presence (RFC 3856 [25]). An element needing location that has a SIP location URI MUST issue a SIP SUBSCRIBE (RFC 6665 [14]) to the location URI. Filters (RFC 4661 [92], RFC 6446 [80] and RFC 6447 [72]) MAY be used to control notification.

An element needing location that has a HELD URI MUST de-reference per RFC 6753 [55].

An access network that provides location by reference MUST supply either a SIP or a HELD location reference URI. Networks that use other protocols must interwork to SIP or HELD. NGCS that receive a location reference and forward location in SIP signaling to another element MUST pass the reference, and not any value that they determine by de-referencing (although the value should be logged). Each element MUST do its own de-reference operation, supplying its credentials to the LIS. It is RECOMMENDED that LISes cache location values and supply the cached values if multiple de-references occur in quick succession, such as when a call is being routed.

In order for a LIS to be NG9-1-1 compliant, it MUST accept credentials traceable to the PSAP Credentialing Agency (PCA) when establishing the TLS connection as sufficient to deliver "dispatch" quality location. The credentials MAY be used by the LIS to authorize delivery of the caller's location, with the required confidence/uncertainty information (when geodetic location is supplied) or civic/sub-civic address-level information (when civic location is supplied), when requested by a PSAP or other authorized entities.

When location is passed by value, processing elements along the path MUST NOT change the location record. If additional location is acquired[15], a new PIDF-LO with a different <Provided-by> element MUST be created and passed in addition to the original location. If the additional location is added before the call arrives at the PSAP, this additional location

[14] A LIS, if it implements the SIP Subscribe/Notify mechanisms for location dereferencing, implements these portions of Presence server as defined in the IETF for the purposes of returning the location information only.

[15] No mechanism to add location to a call within the NGCS before it is delivered to a PSAP is defined in this document.

© Copyright 2011-2022 National Emergency Number Association, Inc.

is added to the call signaling. If the additional location is added after the call is answered by a PSAP, it is included in an Emergency Incident Data Object (EIDO).

Location Conveyance for the Session Initiation Protocol (RFC 6442 [8]) allows for multiple locations being passed so long as they relate to the same target however it does not provide guidance as to how to interpret multiple locations by entities processing such information. While it would be advisable to provide a unique location (or a reference to a unique location), there are nonetheless valid use cases for providing multiple locations in emergency calls presented to the ESInet/NGCS. For example, an Originating Network may provide a device-determined location and a network-determined location, after having performed a sanity check on the device-determined location. Another example is for an Originating Network providing a location information by-value and another location information by-reference. This could be useful for expediting call routing using the location by-value and leaving location updates being performed using the location by-reference. A third example is for an Originating Network providing location information in both civic and geodetic formats. This could be useful in cases where both formats are readily available at call setup time (RFC 5491 [52] should be followed in this case). This document provides guidance on how multiple location information could be presented to and processed in the ESInet/NGCS but does not prescribe how, nor does it assume that Originating Networks implement multiple location information on emergency calls.

RFC 6442 [8] states "A SIP intermediary that adds a locationValue MUST position the new locationValue as the last locationValue within the Geolocation header field of the SIP request". Following this principle, it would be advisable that Originating Networks providing multiple location information in the original INVITE do so by making the top entry the preferred location to use for routing and put the other location information after. The order does not reflect whether the first entry is better, more reliable or more granular; it merely specifies the preferred choice of the Originating Network for location to use for routing. In such case, entities making routing decisions (like the ESRP) COULD simply use the top entry for routing and other downstream entities COULD use other entries for other purposes such as dispatch for example. In addition, an entity MAY opt to inspect the method token value and/or the provided-by token associated with each location object, if available, to make a determination on selecting the location information to use. An Originating Network may also provide a location-source parameter associated with each location information being passed, as defined in *Location Source Parameter for the SIP Geolocation Header Field* (RFC 8787) [201]. This information MAY also be used by downstream entities to make a determination on selecting the location information to use. In addition, the confidence and uncertainty information which may be included in the location information (per RFC 7459) [145] could be considered when selecting from among multiple locations used.

© Copyright 2011-2022 National Emergency Number Association, Inc.

Multiple location information can be expressed in a number of ways. Here are a few examples.

1. Multiple entries in the Geolocation header field

```
Geolocation: <cid:target-a1w@orignet1.com>,
<https://lis.orignet1.com:10236/flwprf232rfk>;loc-src=lrf.orignet1.com
```

2. Multiple Geolocation header fields

```
Geolocation: <cid:target-a1w@orignet1.com>
Geolocation: <https://lis.orignet1.com:10236/flwprf232rfk>;loc-
src=lrf.orignet1.com
```

3. Multiple Location Information within a PIDF-LO

   Refer to the example in section 5.2 of RFC 6442 [8].

There are multiple references to the Geolocation header field in this document. These references MUST be interpreted to include the possibility of multiple location information.

Other than otherwise specified above, the implementation used within the origination and access networks for support of location is out of scope of i3[16].

3.3 Policy (policies)

Policies are stored into and retrieved from a Policy Store using a web service. Section 3.3.1 below describes the "Policy Store Web Service" that facilitates agencies uploading and retrieving policies. Policies are named for the function that the policy affects, (e.g., the RoutePolicy for a queue on an ESRP). A policy (or policy document or policy object) consists of a set of rules and is sometimes termed a "ruleset". A specific Policy ruleset is uniquely identified by the combination of the policy name and the ID of the agency that owns (created) the policy and in some cases, the queue name. The client side of a web service authentication with the Policy Store identifies the agency storing or retrieving Policy rulesets.

The Policy Store only accepts or delivers complete Policy rulesets, not individual rules within a Policy ruleset. The policy retrieved is valid until the expiration time. If the policy is needed for use after expiration, it MUST be retrieved again from the Policy Store. A policy retrieval request MAY return a referral to another Policy Store instead of the requested policy. The referred-to Policy Store might have the policy or might return another referral.

[16] The roles of the access and originating networks in obtaining location for routing and delivery with an emergency call and interactions between such networks is out of scope and subject to SDO work outside NENA as well as regulatory policy.

© Copyright 2011-2022 National Emergency Number Association, Inc.

The standard i3 data rights management system can limit which agencies, agents, or functions are permitted to retrieve policies for another agency. The rights management policy (named "PolicyStore") can also allow an agency to store policies on behalf of another agency.

Policies stored in the Policy Store MUST be signed by the owner of the Policy. A policy document MUST be a JSON Web Signature (JWS) object [171] per Section 5.10. For agencies within an ESInet, a credential traceable to the PCA MUST be used.

3.3.1 Policy Store Web Service

The Policy Store web service stores and retrieves policies (rulesets). The Policy Store accepts a policy document from a policy owner (an agency) or an agency authorized to store policies on behalf of the owner. Policies are identified by the policy type, the identity of the agency whose owns the policy and for Policy Routing Rules, a policyQueueName or an Id. Policy Types come from the Policy Type Registry 10.33 and consist of service names (which are policies that describe the access rights for the service), and policyTypes specified by this document or other NENA standards. The Policy Store provides the policy on request to a policy retriever. The Policy Store does not alter the policy document in any way; it stores it as an octet stream, without performing line-ending conversion, JSON or XML normalization, reformatting, or any other alteration. This allows the policy signature to be verified more efficiently, by avoiding the need to re-canonicalize the JSON.

A policy is represented by a JWS which contains a Policy Object. The Policy Object consists of:

Name	Condition	Description
policyOwner	MANDATORY	ID of the agency or service whose policy is requested. MUST be a FQDN or URI that contains a FQDN
policyType	MANDATORY	Type of the policy. Restricted to the values in the Policy Types registry
policyId	CONDITIONAL, MUST NOT be specified unless policyType is "OtherRoutePolicy"	For "OtherRoutePolicy", this is an arbitrary identifier for the policy

© Copyright 2011-2022 National Emergency Number Association, Inc.

Name	Condition	Description
policyQueueName	CONDITIONAL, MUST NOT be specified unless policyType is "OriginationRoutePolicy" or "NormalNextHopRoutePolicy"	For "OriginationRoutePolicy" or "NormalNextHopRoutePolicy", this is the policyQueueName
policyExpirationTime	OPTIONAL	Policy is not valid after this time
policyRules	MANDATORY	Array of Rules
policyLastModificationTime	CONDITIONAL, MUST be provided on retrieval, ignored on store	Date/Time policy was last modified
description	OPTIONAL	Text description of policy

3.3.1.1 Versions

The Versions entry point of the Policy Store Web Service MUST include, in the "serviceInfo" parameter, the parameter "requiredAlgorithms" whose value is an array of JWS algorithms (as described in 5.10) acceptable to the policy store. The following example is from a policy store whose policy permits only the "EdDSA" algorithm:

```
{
   "fingerprint": "Woof-FurrySuite-v8-8c439e",
   "versions":
      [
         { "major": 6, "minor": 3,
           "vendor": "burby-magic",
           "serviceInfo": { "requiredAlgorithms": [ "EdDSA" ] }
         }
      ]
}
```

The OpenAPI definition of this interface can be found in Appendix E.1. This web service has the following functions:

3.3.1.2 Policies

Retrieves, Stores, Updates and Deletes a Policy ruleset from the common Policy Store. Policies are identified by the policy type, the identity of the agency whose policy is needed and for Policy Routing rules, a policyQueueName and possibly an Identifier. Policy Types come from the Policy Type Registry (Section 10.33) and consist of service names (which

© Copyright 2011-2022 National Emergency Number Association, Inc.

are policies that describe the access rights for the service), and types specified by this document or other NENA standards.

For a GET operation the response is the Policy ruleset. The type, owner, id and/or policyQueueName can be omitted (at least one MUST be provided). This is a "wild-card" response where the set of policies that have the supplied parameter(s) is returned. Limit and start parameters are supported for pagination. The policies retrieved are valid until the expiration time. If the policy is needed for use after expiration, it MUST be retrieved again from the Policy Store.

Instead of returning the policy requested, the response MAY return a referral to another Policy Store that might have the policy via an HTTP 307 Temporary Redirect.

3.3.1.2.1 Retrieve Policies

HTTP method: GET

Resource name .../Policies

Name	Condition	Description
limit	OPTIONAL	Maximum number of results to return
start	OPTIONAL	First item in the page of results, as an ordinal 1-based integer.
policyOwner	CONDITIONAL, at least one of policyType, policyOwner, policyId or policyQueueName MUST be provided	ID of the agency or service whose policy is requested. MUST be a FQDN or URI that contains a FQDN
policyType	CONDITIONAL, at least one of policyType, policyOwner, policyId or policyQueueName MUST be provided	Type of the policy. Values are limited to names in the Policy Types registry
policyId	CONDITIONAL, at least one of policyType, policyowner, policyId or policyQueueName MUST be provided. If policyType is specified, MUST NOT be specified unless policyType is "OtherRoutePolicy"	For "OtherRoutePolicy", this is the id mentioned in an InvokePolicyAction

© Copyright 2011-2022 National Emergency Number Association, Inc.

Name	Condition	Description
policyQueueName	CONDITIONAL, at least one of policyType, policyowner, policyId or policyQueueName MUST be provided. If policyType is specified, MUST NOT be specified unless policyType is "OriginationRoutePolicy" or "NormalNextHopRoutePolicy"	For PRRs, this is the policyQueueName

Status Codes

200	Policies found
307	Temporary Redirect
451	Unknown or bad Policy Type
452	Unknown or bad Agency Name
453	Not available here, no referral available
454	Unspecified Error

On a successful GET, a PolicyArray is returned:

PolicyArray

Name	Condition	Description
count	MANDATORY	Number of items in the array
totalCount	MANDATORY	Total number of items found
policies	MANDATORY	Array of Policy objects, each as a JWS

3.3.1.2.2 Store Policy

Initiates the creation of a Policy ruleset in the Policy Store. The POST has a request body containing the Policy as a JWS.

Following a POST, the Policy Store MUST confirm that the policyExpirationTime is in the future, the size of the received policy exactly matches the size specified in policySize, the structure and contents of the document is well-formed and conformant, for Policy Routing Rules that each rule has a unique id, and verify the signature of the JWS.

HTTP method: POST

© Copyright 2011-2022 National Emergency Number Association, Inc.

Resource name .../Policies

The request body contains the policy as a JWS

Status codes

201	Policy successfully created
434	Signature Verification Failure
436	Duplicate or Invalid Priority
437	Bad Policy Structure
451	Unknown or bad Policy Type
452	Unknown or bad Agency Name
454	Unspecified Error
460	Bad PolicyExpirationTime

3.3.1.2.3 Update Policy

Initiates the update of a Policy ruleset in the Policy Store. This function's parameters include the name of the policy, the agency or service whose policy is being updated, for PRRs, the policyQueueName or policyId. The request body contains the replacement policy as a JWS.

When processing an Update request, the Policy Store MUST confirm that the policyExpirationTime is in the future, the size of the received policy exactly matches the size specified in policySize, the structure and contents of the document is well-formed and conformant, for Policy Routing Rules that each file has a unique ID, and verify the signature of the JWS.

HTTP method: PUT

Resource name .../Policies

The request body contains the replacement policy as a JWS

Parameters:

Name	Condition	Description
policyOwner	MANDATORY	ID of the agency or service owning the policy(ies). MUST be a FQDN or URI that contains a FQDN
policyType	MANDATORY	Type of the policy

© Copyright 2011-2022 National Emergency Number Association, Inc.

Name	Condition	Description
policyId	CONDITIONAL, MUST be provided if policyType is "OtherRoutePolicy"	For "OtherRoutePolicy", the id of the policy mentioned in the InvokePolicyAction
policyQueueName	CONDITIONAL, MUST be provided policyType is "OriginationRoutePolicy" or "NormalNextHopRoutePolicy"	For PRRs, this is the policyQueueName

Status Codes

200 Policy successfully updated
404 Not found
434 Signature Verification Failure
436 Duplicate or Invalid Priority
437 Bad Policy Structure
451 Unknown or bad Policy Type
452 Unknown or bad Agency Name
454 Unspecified Error
460 Bad PolicyExpirationTime

3.3.1.2.4 Delete Policy

Deletes a Policy ruleset in the Policy Store. The parameters are the name of the policy and the agency/service whose policy is being deleted and for PRRs, the policyQueueName or policyId.

HTTP method: DELETE

Resource name …/Policies

Parameters:

Name	Condition	Description
policyOwner	MANDATORY	ID of the agency or service whose policy is requested. MUST be a FQDN or URI that contains a FQDN
policyType	MANDATORY	Type of the policy

© Copyright 2011-2022 National Emergency Number Association, Inc.

Name	Condition	Description
policyId	CONDITIONAL, MUST be provided if policyType is "OtherRoutePolicy"	For "OtherRoutePolicy", the id of the policy mentioned in the InvokePolicyAction
policyQueueName	CONDITIONAL, MUST be provided policyType is "OriginationRoutePolicy" or "NormalNextHopRoutePolicy"	For PRRs, this is the policyQueueName

Status Codes

200	Policy successfully deleted
404	Not found
451	Unknown or bad Policy Type
452	Unknown or bad Agency Name
454	Unspecified Error

3.3.1.3 Policy Enums

Returns a list of policy names available in the store for a specific agency/service. The type, owner, policyId and/or policyQueueName can be omitted (at least one MUST be provided). This is a "wild-card" response where the set of policies that have the supplied parameter(s) is returned. Limit and start parameters are supported for pagination. The enumeration includes only those policies that are actually stored in this specific instance of the Policy Store.

3.3.1.3.1 Enumerate Policies

HTTP method: GET

Resource name .../PolicyEnums

Parameters

Name	Condition	Description
limit	OPTIONAL	Maximum number of results to return
start	OPTIONAL	First item in the page of results, as an ordinal 1-based integer.

© Copyright 2011-2022 National Emergency Number Association, Inc.

Name	Condition	Description
policyOwner	CONDITIONAL, at least one of policyOwner, policyType, policyQueueName, policyId or policiesUpdatedSince MUST be provided	ID of the agency or service whose policy is requested. MUST be a FQDN or URI that contains a FQDN
policyType	CONDITIONAL, at least one of policyowner, policyType, policyQueueName, policyId or policiesUpdatedSince MUST be provided	Type of the policy. MAY be "*" for all policy types
policyId	CONDITIONAL, at least one of policyowner, policyType, policyQueueName, policyId or policiesUpdatedSince MUST be provided	For "OtherRoutePolicy", the id of the policy mentioned in the InvokePolicyAction
policyQueueName	CONDITIONAL, at least one of policyowner, policyType, policyQueueName, policyId or policiesUpdatedSince MUST be provided	For PRRs, this is the policyQueueName
policiesUpdatedSince	CONDITIONAL, at least one of policyowner, policyType, policyQueueName, policyId or policiesUpdatedSince MUST be provided	Query returns all policies having the time of creation or last modification greater than policiesUpdatedSince

© Copyright 2011-2022 National Emergency Number Association, Inc.

On a successful GET, a PolicyEnumArray is returned:

PolicyEnumArray

Name	Condition	Description
count	MANDATORY	Number of items in the array
totalCount	MANDATORY	Total number of items found
policyEnums	MANDATORY	Array of PolicyEnum objects

PolicyEnum (for each policy)

Name	Condition	Description
policyType	MANDATORY	The type of the policy.
policyOwner	MANDATORY	The policy owner of interest. MUST be a FQDN or URI that contains a FQDN
policyId	CONDITIONAL, MUST be provided for "OtherRoutePolicy"	Id of the policy
policyQueueName	CONDITIONAL, MUST be provided for "NominalNextHopRoutePolicy"	For "RoutePolicy", this is the policyQueueName
policyExpirationTime	MANDATORY	The expiration time of the policy
policyLastModificationTime	MANDATORY	Date/Time of last modification

Status Codes

200 Policies enumerations found
404 Not found
451 Unknown or bad Policy Type
452 Unknown or bad Agency/Service Name
454 Unspecified Error

3.3.2 Policy Store Replication

The Policy Store is replicated and distributed. There is a single authoritative master store for each agency (policy owner). There MAY be one or more replicas in other Policy Stores of the policies for any given agency. Each Policy Store that is authoritative for the policies of one or more agencies is provisioned with a list of replicas that are authorized to store policies from each agency. Each replica is provisioned with a list of agencies for which it serves as replica and the authoritative master policy store for each. A replica uses the

© Copyright 2011-2022 National Emergency Number Association, Inc.

RetrievePolicy function to get policies from the master Policy Store, and refreshes them automatically before they expire. EnumeratePolicy MAY be used to determine which agency's policies are stored in the Policy Store.

As an optimization, the replica MAY make use of the policiesUpdatedSince parameter:

policiesUpdatedSince MAY be used as a poll to maintain an up-to-date replica, rather than waiting for expiration times of individual policies (since a policy owner might update a policy prior to expiration). Use of policiesUpdatedSince is RECOMMENDED for replicas of policies that could reasonably be changed unexpectedly, such as in a disaster situation.

The Policy Store is replicated and distributed. There is a single authoritative master store for each agency (policy owner). There MAY be one or more replicas in other Policy Stores of the policies for any given agency. Each Policy Store that is authoritative for the policies of one or more agencies is provisioned with a list of replicas that are authorized to store policies from each agency. Each replica is provisioned with a list of agencies for which it serves as replica and the authoritative master policy store for each. A replica uses the Policies GET function to get policies from the master Policy Store and refreshes them automatically before they expire. PolicyEnums MAY be used to determine which agency's policies are stored in the Policy Store.

The PolicyEnums function is also useful to maintain a referral service to distribute the Policy Store. Policy Stores MAY refer queries to another Policy Store. To do so, they maintain a map of which Policy Stores have what policies. The mapping MAY be provisioned or learned via the PolicyEnums function (with a list of other Policy Stores provisioned in a specific Policy Store).

3.3.3 Route Policy Syntax

This section describes the syntax and semantics of the policy language used for making call routing decisions.

A policy document is a JWS; the payload is a JSON object conformant to the 'Policy' type in Appendix E.1.1 with rules conforming to the 'Rule' object. Policy documents are carried using the MIME type of Application/EmergencyCallData.auth-policy+json. A policy document is composed of a set of rules and an optional description. Each rule is a JSON object containing the following members:

- "id" (REQUIRED): a string containing an ID for the rule; the value MUST be unique within the ruleset
- "priority" (REQUIRED): an integer greater than or equal to zero that MUST be unique within the ruleset; this is the rule's priority

© Copyright 2011-2022 National Emergency Number Association, Inc.

- "conditions" (OPTIONAL): an object that MAY contain one or more Condition objects (Section 3.3.3.1 below)
- "actions" (REQUIRED): an object that MUST contain one or more Action objects (Section 3.3.3.1 below)
- "description" (OPTIONAL): a string that describes the rule

Within a rule, the "Conditions" object evaluates to 'true' or 'false'. If it evaluates to 'true' then the "actions" part of the rule is eligible to be executed. Because multiple rules might have "Condition" parts that evaluate to 'true', each rule has an associated priority value. A higher (numerically greater) value takes precedence over a rule with a lower value. When more than one rule has a "Conditions" section that evaluates to 'true', only the rule with the largest priority value has its actions section executed. Priority 0 is the lowest priority; a rule with priority 0 is only executed if no other rule's "conditions" evaluate to 'true'. Each rule also has an ID, which is a string unique to the ruleset.

In a Route Policy, an omitted "Conditions" section evaluates to 'true'; this permits constructing default or "catch-all" rules that are executed only if no other rule matches. Normally, such rules have an extremely low priority value, e.g., 0.

A Route Policy document MUST be a JWS [171] as per Section 5.10 and MUST have a payload conforming to Appendix E.10.

A routing element MUST verify the JWS signature before executing the rules. The Policy Store is REQUIRED to store and retrieve Route Policy documents byte-for-byte unaltered (so that the JWS extracted is the exact same octet stream stored, and calculates the exact same digest). If the JWS signature verification fails, the policy MUST NOT be executed. Any element encountering a failed JWS signature verification SHOULD file a Policy Discrepancy Report (Section 3.7.13) against the policy owner and MAY file a Policy Store Discrepancy Report (Section 3.7.4) against the Policy Store.

3.3.3.1 Conditions

This section describes the "Conditions" part of the rule. "Conditions" is an array of zero or more condition objects (listed in the following subsections), that MAY contain a "negation" member that inverts the condition sense. Several conditions require that the ESRP use the SIP-based notification mechanism described in RFC 6665 [14] to be aware of the state or condition of an external entity (such as a service or queue), or perform a Location to Service Translation (LoST) query and store the resulting URI in a variable.

A condition object contains the following members:

- conditionType: a string which MUST exist and be set to the specific condition type.

© Copyright 2011-2022 National Emergency Number Association, Inc.

- negation: an OPTIONAL Boolean that when set to 'true' inverts the condition sense. When "negation" exists and is set to 'true', it reverses the evaluation of the "Conditions" object; when set to 'false' or omitted it has no effect.
- description: an OPTIONAL string containing a description of the condition.
- Other condition-specific members as described in the below subsections.

When "Conditions" contains more than one condition object, they are evaluated using a logical AND: if they all evaluate as 'true', the "Conditions" evaluates as 'true'; if any evaluate as 'false', the "Conditions" evaluates as 'false'. The exception is "TimePeriodCondition": all "TimePeriodCondition" objects in a rule are evaluated with an implicit OR. Logically, each condition other than "TimePeriodCondition" in a rule is evaluated; if they all evaluate as 'true' and any "TimePeriodCondition" within the rule evaluates to 'true', then the "Conditions" evaluates to 'true'.

After evaluation of the contained condition object(s), if the "negation" member is present and set to 'true', the evaluation is reversed.

If a ruleset has no conditions that evaluate to 'true', the ESRP MUST treat this as a fatal error (see Section 4.2.1.6).

3.3.3.1.1 Time Period Condition

"TimePeriodCondition" allows a rule to make decisions based on the time, date, and time zone. The following members are defined for use within a "TimePeriodCondition" object:

dateStart: Start of interval (Timestamp, see Section 2.3). This member is MANDATORY.

dateEnd: End of interval (Timestamp). This member is MANDATORY.

timeStart: Start of time interval in a particular day. It uses the partial-time data type as described in Section 5.6 of RFC 3339 [135], interpreted as having the same offset from UTC as found in dateStart and dateEnd. This member is OPTIONAL. The default value is "00:00:00".

timeEnd: End of time interval in a particular day. It uses the partial-time data type as described in Section 5.6 of RFC 3339 [135], interpreted as having the same offset from UTC as found in dateStart and dateEnd. This attribute is OPTIONAL; if specified MUST be greater than the value of timeStart. The default value is 23:59:59.

weekdayList: List of days of the week. This member is optional. The "weekdayList" member specifies a comma-separated list of days of the week:

- "MO" indicates Monday,
- "TU" indicates Tuesday,

© Copyright 2011-2022 National Emergency Number Association, Inc.

- "WE" indicates Wednesday,
- "TH" indicates Thursday,
- "FR" indicates Friday,
- "SA" indicates Saturday, and
- "SU" indicates Sunday.

These values are not case-sensitive. Whitespace after a comma is permitted.

An ESRP or other entity executing a policy MUST ignore an invalid value in a member (e.g., a timeStart or timeEnd with an hour greater than 24, or minutes or seconds greater than 60, or hour set to 24 with minutes or seconds greater than 0) but SHOULD generate a Discrepancy Report against the policy owner (Section 3.7.13) and MAY file a DR against the Policy Store (Section 3.7.4). A Policy Store MUST reject as an error an attempt to store or update a policy containing an invalid value. A Policy Store MAY also file a Discrepancy Report against the policy owner.

3.3.3.1.1.1 Examples of "TimePeriodCondition"

The following examples illustrate the "TimePeriodCondition" object:

```
{
    "conditionType": "TimePeriodCondition",

    "description": "Example Time Rule 1
    Rule applies on weekdays (Monday through Friday)
    between 8:00 AM and 6:00 PM during the period
    from January 12th, 2017 8:30 AM Eastern Standard Time
    until January 1st, 2018 6:30 PM Eastern Standard Time
    NOT accounting for Daylight Saving Time:",

    "dateStart":    "2017-01-12T08:30:00-05:00",
    "timeStart":    "08:00",
    "timeEnd":      "18:00",
    "weekdayList":  "MO,TU,WE,TH,FR",
    "dateEnd":      "2018-01-01T18:30:00-05:00"
}


{
    "conditionType": "TimePeriodCondition",

    "description": "Example Time Rule 2
    Rule applies on weekdays (Monday through Friday)
    between 8:00 AM and 6:00 PM during the period
    from January 1st, 2018 12:01 AM Eastern Standard Time
    until December 31st, 2019 11:59 PM Eastern Standard Time
    adjusting for Daylight Saving Time (2:00 AM on the second
    Sunday in March until 2:00 AM on the first Sunday of
    November) during the period:
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
    Standard Time period at start of 2018:",

    "dateStart":    "2018-01-01T00:01:00-05",
    "timeStart":    "08:00",
    "timeEnd":      "18:00",
    "weekdayList":  "MO,TU,WE,TH,FR",
    "dateEnd":      "2018-03-11T01:59:59-05:00"
}


{
    "conditionType": "TimePeriodCondition",

    "description": "Daylight Saving Time period of 2018:",

    "dateStart":   "2018-03-11T02:00:00-04:00",
    "timeStart":   "08:00",
    "timeEnd":     "18:00",
    "weekdayList": "MO,TU,WE,TH,FR",
    "dateEnd":     "2018-11-04T01:59:59-04"
}


{
    "conditionType": "TimePeriodCondition",

    "description": "Standard time period winter 2018-2019:",

    "dateStart":   "2018-11-04T02:00:00-05:00",
    "timeStart":   "08:00",
    "timeEnd":     "18:00",
    "weekdayList": "MO,TU,WE,TH,FR",
    "dateEnd":     "2019-03-10T01:59:59-05:00"
}


{
    "conditionType": "TimePeriodCondition",

    "description": "Daylight Saving Time period of 2019:",

    "dateStart":   "2019-03-10T02:00:00-04",
    "timeStart":   "08:00",
    "timeEnd":     "18:00",
    "weekdayList": "MO,TU,WE,TH,FR",
    "dateEnd":     "2019-11-03T01:59:59-04:00"
}


{
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
        "conditionType": "TimePeriodCondition",

        "description": "Standard time period late 2019:",

        "dateStart":    "2019-11-03T02:00:00-05:00",
        "timeStart":    "08:00",
        "timeEnd":      "18:00",
        "weekdayList":  "MO,TU,WE,TH,FR",
        "dateEnd":      "2019-12-31T23:59:59-05:00"
    }
```

The following aspects need to be considered:

1. By default, if all the OPTIONAL members are omitted, the TimePeriodCondition is valid for the whole duration from "dateStart" to "dateEnd" inclusive.
2. The "weekdayList" member comes into effect only if the period from "dateStart" until "dateEnd" is long enough to accommodate the specified values, otherwise it is ignored.
3. Any "weekdayList" values that do not correspond to expected values MUST be ignored.
4. Each "timeStart" and "timeEnd" member MUST contain a single value. If "timeStart" is later than "timeEnd", both "timeStart" and "timeEnd" SHALL be ignored.
5. Multiple "TimePeriodCondition" objects MAY be included in a rule. If multiple "TimePeriodCondition" objects are present, each is evaluated independently (an implicit "or").
6. The time is specified with a timezone offset (i.e., in local time with the offset from UTC); rules need to consider any local daylight-saving changes. Multiple time period specifications MAY be used for this purpose.
7. Since rules with time elements may have an end time, updates to rules may be required occasionally to maintain the desired effect.

3.3.3.1.2 SIP Header Condition

"SipHeaderCondition" tests a SIP header field in the INVITE or MESSAGE of a call (such as "From", "To", "Contact", etc.).

The "SipHeaderCondition" object has three members:

- "field", which MUST exist and be set to the name of a SIP header field (e.g., "Recv-Info"); note that the value does not include the colon which follows a header field name in a message. The value MUST be the full name of the header field; it matches the full or abbreviated name of the header field in the SIP message.
- "operator", which MUST exist and be set to one of:

© Copyright 2011-2022 National Emergency Number Association, Inc.

- "EQ" for an equality match,
- "SS" for a substring match, or
- "IS" for a registry-defined match.

- "content", which MUST be present. If "operator" is set to "EQ" or "SS", this member contains a string against which the specified header field value is compared, either for equality or as a substring. If "operator" is set to "IS", this member MUST be set to an entry in the "SIPheader 'Is' Operator conditions" registry (Section 10.15).

An equality match compares the value of the "content" member against the value of the specified header field, including any parameters. A substring match tests if the value of the "content" member is present anywhere in the header field value, including parameters. Both equality and substring matches are case-insensitive.

The "IS" operator uses a registry (See "SIPheader 'Is' Operator conditions", Section 10.15) The "content" member is set to a value contained in the registry. This operator tests the header field for the condition is specified by the "content" value per the registry.

"SipHeaderCondition" evaluates to 'false' if "operator" is "EQ" or "SS" and the specified header field is not found in the SIP INVITE or MESSAGE.

3.3.3.1.3 Additional Data Condition

"AdditionalDataCondition" tests the SIP INVITE or MESSAGE of the call to check if it contains an Additional Data block that meets a specified condition. At minimum, ESRPs access and evaluate against the condition criteria all Additional Data blocks that are conveyed by value or by reference via Call-Info header fields. It is implementation dependent if the ESRP also performs an ECRF query for URIs for Additional Data associated with a location and then dereferences those URIs, or queries IS-ADRs, to access and evaluate further Additional Data blocks against the Additional Data condition. No mechanisms currently exist, however, for differentiating these data blocks in the rule. This will be subject to review in a subsequent version of this document. See Sections 4.2.2.3 ECRF interface, 4.2.2.5 Additional Data Interface, 4.3.3.4 Service to access Additional Data for a location, and 4.11.1 Identity Searchable Additional Data Repository (IS-ADR).

The "AdditionalDataCondition" object has four members:

- "type", which MUST exist and be set to a value consisting of "EmergencyCallData", a dot, and a block type contained in the IANA Emergency Call Data Types Registry [179].

© Copyright 2011-2022 National Emergency Number Association, Inc.

- "element" which value is the name of one of the elements in the specified Additional Data block; this member MUST be omitted when "operator" is set to "exists" or "missing" and is MANDATORY otherwise.
- "operator", which MUST exist and be set to one of:
    - "exists", which evaluates as 'true' if the specified Additional Data block exists in the incoming message;
    - "missing", which evaluates as 'true' if the specified Additional Data block does not exist in the incoming message;
    - "EQ" (equals), which checks for equality (case-insensitive) between the string in "content" and the element contents;
    - "SS" (substring), which checks if the string in "content" is contained in the element (case-insensitive);
    - "NE" (not equal to), which is the inverse of "EQ";
    - "GT" (greater than), which checks if the string in "content", treated a numeric or date value, is greater than the element contents;
    - "LT" (less than), which checks if the string in "content", treated a numeric or date value, is less than the element contents;
    - "GE" (greater than or equal to), which checks if the string in "content", treated a numeric or date value, is greater than or equal to the element contents;
    - "LE" (less than or equal to), which checks if the string in "content", treated a numeric or date value, is less than or equal to the element contents;

      If the value in the Additional Data Block element being processed does not evaluate to a number or a date, GT/LT/GE/LE evaluate to 'false'. String comparisons are case-insensitive. If the specified Additional Data Block does not exist or does not contain the specified element, all operators other than "missing" evaluate to 'false'.
- "content", the value of which is compared with the value of the specified element of the specified Additional Data block, using the test specified by "operator"; this member MUST be omitted when "operator" is "present" or "missing" and is MANDATORY otherwise.

A typical use for this condition is to route based on the class of service components, or to route VEDS calls to a VEDS-equipped PSAP.

3.3.3.1.3.1 Examples of "AdditionalDataCondition"

The following example tests if the "EmergencyCallData.ServiceInfo" block's <ServiceType> element (analogous to Class of Service in legacy E9-1-1) indicates the call was placed via a

© Copyright 2011-2022 National Emergency Number Association, Inc.

relay service (which would be the case if the call was placed via a sign language relay/interpretation service or a telematics service that provides a human on the call):

```
{
    "conditionType": "AdditionalDataCondition",
    "type":          "EmergencyCallData.ServiceInfo",
    "operator":      "EQ",
    "element":       "ServiceType",
    "content":       "relay"
}
```

The following example tests if a call contains an <EmergencyCallData.VEDS> block, indicating the call is an NG-AACN call:

```
{
    "conditionType": "AdditionalDataCondition",
    "type":          "EmergencyCallData.VEDS",
    "operator":      "exists",
}
```

The following example tests if a call contains an <EmergencyCallData.VEDS> block (which indicates the call is an NG-AACN call) containing a 'VehicleFinalRestOrientationCategoryCode' attribute with a value other than 'Normal' (indicating that the vehicle's final resting orientation is abnormal, e.g., on a side or roof or end):

```
{
    "conditionType": "AdditionalDataCondition",
    "type":          "EmergencyCallData.VEDS",
    "operator":      "NE",
    "element":       "VehicleFinalRestOrientationCategoryCode",
    "content":       "Normal"
}
```

3.3.3.1.4 MIME Body List Condition

"MimeBodyCondition" tests if an incoming call's SIP INVITE or MESSAGE has a body part with a specified MIME type.

The "MimeBodyCondition" object MUST contain a "mimeList" member, which is an array of strings. Each string is a MIME media type and subtype (e.g., "text/plain") from the IANA registry [181]. The values in the array are compared with the content types in the body of the SIP INVITE or MESSAGE. A "MimeBodyCondition" object evaluates to 'true' if any of the call's body parts is of a type contained in the array (i.e., the MIME type and subtype of each body part of the SIP INVITE or MESSAGE is compared against each value in the array using a logical OR).

© Copyright 2011-2022 National Emergency Number Association, Inc.

3.3.3.1.5 Location Condition

The location used for the routing of a call can be tested using the "LocationCondition" object, which is derived from the location-based condition elements specified in RFC 6772 [108].

The "LocationCondition" object MUST contain at least one "location" child object. The "LocationCondition" object evaluates to 'true' if any of its child "location" objects evaluate to 'true' when tested against the location used for routing of the call; i.e., multiple "location" child objects in a "LocationCondition" object are combined using a logical OR.

Four members are defined for use in a "location" child object:

- "lo": A "location" child object MUST contain a "lo" member. The value is a PIDF-LO (properly escaped for inclusion in a JSON object).
- "profile": The "profile" member MUST exist and be set to "geodetic" or "civic". This member indicates the location profile of the "location" object in which it appears. The semantics of the two location profiles, "geodetic" and "civic", are derived from RFC 6772 [108], Sections 4.1 and 4.2. The profile describes under what conditions a "location" child object evaluates to 'true' (i.e., the "profile" value specifies how to test the PIDF-LO contained in the "lo" member against the location used for routing of the call).
    - "geodetic": Using the semantics described in RFC 6772 [108] Section 4.1, this profile tests if the location used for routing the call is entirely within a specified circle.

      Note that if the location used for routing is provided in geodetic form, it could be specified as a point, arc-band, circle, or other shape, which must be entirely contained in the circle specified in the "lo" member for the "location" object to evaluate to 'true'. If the call's location for routing is not specified in geodetic form, the "location" object evaluates to 'false'.
    - "civic": Using the semantics described in RFC 6772 [108], Section 4.2, this profile tests the location used for routing the call against a set of civic address elements. The civic address elements of the PIDF-LO contained in the "lo" member are compared against the same elements of the location used for routing the call. Per RFC 6772 [108], Section 4.2, each civic address element in the "lo" member MUST exist in the location used for routing the call, and the values MUST be identical on an octet-by-octet basis (case-sensitive, no normalizations of abbreviations, prefixes, suffixes, etc.) If the call's location for routing is not specified in civic form, the "location" object evaluates to 'false'.

© Copyright 2011-2022 National Emergency Number Association, Inc.

- "label": This member allows a human-readable description to be added to each "location" child object. It is OPTIONAL.
- "lang": This member contains a language tag providing further information for rendering of the content of the "label" member. It is OPTIONAL. The "lang" member MUST NOT be present unless the "label" member is also present.

The "LocationCondition" and the "location" objects both allow extension points by using an embedded "extension" child object. If an extension is not understood by the entity evaluating the conditions, then this condition evaluates to 'false'. A "LocationCondition" is considered 'true' if any of the "location" objects understood by the condition evaluator is 'true'.

3.3.3.1.6 Call Suspicion Condition

"CallSuspicionCondition" tests the suspicion score of the call.

If the SIP INVITE or MESSAGE contains a Call-Info header field with a 'purpose' parameter set to "emergency-CallSuspicion", the value specified in the header field is considered an integer suspicion score.

"CallSuspicionCondition" evaluates this suspicion score. The "CallSuspicionCondition" object has two members: "scoreFrom" and "scoreTo", both of which MUST be present and MUST contain an integer value. The "CallSuspicionCondition" object evaluates to 'true' if the call's suspicion score is greater than or equal to the value of "scoreFrom and less than or equal to the value of "scoreTo".

If the call does not have a suspicion score, or the suspicion score cannot be determined as an integer, the suspicion score is considered to be zero.

3.3.3.1.7 Security Posture Condition

"SecurityPostureCondition" tests the current security posture of a service or agency. Security Posture is one part of Service State.

The "SecurityPostureCondition" object has three members:

- "service", which MUST exist. It contains one of Service Name, Service Identifier, or Agency Identifier. If specified by Service Name, it MUST be an entry in the Service Names Registry (Section 10.11) and MUST NOT be PSAP. The address to subscribe for Service State can be found using the Service/Agency Locator, which contains the subscription address for ServiceState.
- "condition", which MUST exist and be set to "EQ" (equals) or "NE" (not equal to).
- "value", which MUST exist and be set to an entry in the Security Posture Registry (see Section 10.18).

© Copyright 2011-2022 National Emergency Number Association, Inc.

The "SecurityPostureCondition" compares the current state of the Security Posture for the specified service or agency against the value specified in the "value" member. It evaluates to 'true' if the values are the same and the "condition" member is "EQ", or the values are not the same and the "condition" member is "NE", and 'false' otherwise. If the ESRP is unable to subscribe to the Service State of the specified service or agency at the specified FQDN, the security posture is treated as "Green".

Presence of this condition implies that the ESRP subscribes to the Service State event package for the specified service or agency at the specified domain. Implementations MAY preprocess rulesets to arrange these subscriptions in advance.

3.3.3.1.8 Queue State Condition

"QueueStateCondition" tests the current state of a queue.

The "QueueStateCondition" object has three members:

- "queue": The "queue" member MUST exist and be set to a queue URI. The entity identified by the URI MUST support the QueueState event package (see Section 4.2.1.3).
- "condition": The "condition" member MUST exist and be set to "EQ" or "NE".
- "value": The "value" member MUST exist and be set to an entry in the Queue State Registry (see Section 10.17).

"QueueStateCondition" compares the current state of the specified queue against the value specified in the "value" member. It evaluates to 'true' if the values are the same and the "condition" member is "EQ", or the values are not the same and the "condition" member is "NE", and 'false' otherwise. If the ESRP is unable to subscribe to a queue's state, it is treated as "unreachable".

Presence of this condition implies that the ESRP subscribes to queue state notification for the specified queue. Implementations MAY preprocess rulesets to arrange these subscriptions in advance.

3.3.3.1.9 LoST Service URN Condition

"LostServiceUrnCondition" causes a route query to be performed for a specified service URN using the location for routing of the call, and as a side effect sets the "Normal-NextHop" variable.

The "LostServiceUrnCondition" object MUST contain one "urn" member, which MUST be set to a Service URN (e.g., starting with either "urn:service:" or "urn:emergency:service:"). The condition causes a LoST query to be sent to the ECRF using the location for routing in the call and the specified Service URN. The "LostServiceUrnCondition" object evaluates to

© Copyright 2011-2022 National Emergency Number Association, Inc.

'true' if the query is successful and 'false' if not. If the query succeeds, the resulting URI is stored in the "Normal-NextHop" variable. The value of "Normal-NextHop" is available to the rule evaluation system in the Normal-NextHop Condition (Section 3.3.3.1.14) and the Invoke Policy Action (Section 3.3.3.2.5). If the LoST query fails, then the evaluation of this rule stops and the value of "Normal-NextHop" is undefined. (Since this rule's conditions evaluate to 'false', the next lower priority rule that evaluates to 'true' is performed.).

When the LostServiceURN condition is used, the rule SHOULD contain an Invoke Policy Action (Section 3.3.3.2.5) using a PolicyType of "NormalNexthopRoutePolicy" (see section 3.3.3.2.5.

If the LoST response specifies an 'Expires' attribute of 'NO-CACHE', the ESRP MAY retain the value of "Normal-NextHop" for the entirety of rule evaluation for the call instead of re-querying the ECRF for every rule evaluation containing a LostServiceURN condition with the same query parameters. Otherwise, the ESRP MUST respect the expiry of the LoST response in processing this condition.

Entirety of rule evaluation for the call means while the ESRP is evaluating the call, i.e., until the ESRP receives a 200 OK in response to its forward of the INVITE or MESSAGE, or until it generates a 600 Busy Everywhere towards the caller. Rule evaluation includes an Invoke Policy Action.

3.3.3.1.10 Service State Condition

The "ServiceStateCondition" tests the current Service State of service.

The "ServiceStateCondition" object has three members:

- "service", which MUST exist. It contains one of Service Name, Service Identifier or Agency Identifier. If specified by Service Name, it MUST be an entry in the Service Names Registry (Section 10.11) and MUST NOT be PSAP. The address to subscribe for Service State can be found using the Service/Agency Locator, which contains the subscription address for ServiceState.
- "condition": The "condition" member MUST exist and be set to "EQ" or "NE".
- "value": The "value" member MUST exist and be set to an entry in the Service State Registry (see Section 10.12).

"ServiceStateCondition" compares the current service state of the specified service at the specified FQDN against the value specified in the "value" member. It evaluates to 'true' if the values are the same and the "condition" member is "EQ", or the values are not the same and the "condition" member is "NE", and 'false' otherwise. If the ESRP is unable to subscribe to the service state of the specified service at the specified FQDN, it is treated as "unreachable".

© Copyright 2011-2022 National Emergency Number Association, Inc.

Presence of this condition implies that the ESRP subscribes to Service state notification for the specified service. Implementations MAY preprocess rulesets to arrange these subscriptions in advance.

3.3.3.1.11 Call Source Condition

"CallSourceCondition" tests the call's source network. CallSource (as defined in the Via header fields of the INVITE) is interpreted by the ESRP to ignore intra-ESInet Vias and other intermediaries. CallSource SHOULD be the ESRP's best determination of the domain of the originating network that handled the call. If there is more than one, the last originating network or service provider prior to the ESInet SHOULD be used. If there are no originating networks, the ESRP uses the domain of the caller as the Call Source. Note that if the call is routed through multiple ESInets, it may be difficult to determine the CallSource within downstream ESInets. Since routing through multiple ESInets normally only occurs in misroute situations, rules using CallSource are unlikely to be effective in these circumstances.

The "CallSourceCondition" object contains two members:

- "operator" which MUST exist and be set to "EQ" (equals), "SS" (substring), or "NE" (not equal to). String comparisons are case-insensitive.
- "content" which MUST exist. This is the value to be compared with the ESRP's determined Call Source value using the test indicated by "operator".

3.3.3.1.12 Body Part Condition

"BodyPartCondition" tests an element or member within an XML or JSON-formatted body part. This capability MAY be used to route based on parameters within a CAP message. (see also the CAP Condition in Section 3.3.3.1.17, which tests for specific CAP elements)

"BodyPartCondition" contains four members:

- "contentType" which MUST exist and be set to a MIME media (content) type and subtype (e.g., "text/plain") in the IANA registry [181], although the condition is only effective for types that contain data formatted using XML or JSON.
- "element" which MUST exist. This is the name of an element or member in the specified body part; this member is omitted when "operator" is "exists" and MANDATORY otherwise.
- "operator" which MUST exist and be set to one of:
  - "exists",
  - "missing",
  - "EQ" (equals),
  - "SS" (substring),

© Copyright 2011-2022 National Emergency Number Association, Inc.

- "NE" (not equal to),
- "GT" (greater than),
- "LT" (less than),
- "GE" (greater than or equal to), or
- "LE" (less than or equal to).

The "exists" operator evaluates to 'true' if the element or member specified in the "element" member exists in a body part of the specified type in the incoming message, and 'false' otherwise. The "missing" operator evaluates to 'true' if the element or member specified in the "element" member does not exist in any body part of the specified type in the incoming message, and 'false' otherwise. If the value in the body part element or member being processed does not evaluate to a number or date, GT/LT/GE/LE evaluate to 'false'. String comparisons are case-insensitive.

- "content", which MUST exist. This is the value to be compared with the value of the specified element or member of the first body part of the specified type, using the specified comparison operator; this member is omitted when "operator" is "present" or "missing" and MANDATORY otherwise.

Note that the operators "missing" and "exists" potentially test every body part of the specified type, while the comparison operators only test the first occurrence of the specified element or member in the first body part of the specified type in which the element or member appears.

Example Body Part test:

The following example tests an incoming message to see if the body contains a CAP payload with a <msg_status> element set to "Actual", and a <severity> element set to "Extreme", and a <certainty> element set to "High":

```
{
    "conditionType": "BodyPartCondition",
    "contentType":   "application/common-alerting-protocol+xml",
    "element":       "msg_status",
    "operator":      "EQ",
    "content":       "Actual"
},
{
    "conditionType": "BodyPartCondition",
    "contentType":   "application/common-alerting-protocol+xml",
    "element":       "severity",
    "operator":      "EQ",
    "content":       "Extreme"
},
{
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
        "conditionType": "BodyPartCondition",
        "contentType":   "application/common-alerting-protocol+xml",
        "element":       "certainty",
        "operator":      "EQ",
        "content":       "High"
    }
```

3.3.3.1.13 Request URI Condition

"RequestUriCondition" tests the Request-URI in the call's SIP INVITE or MESSAGE. A call's Request-URI is most frequently "urn:service:sos", but can contain child elements (e.g., "urn:service:sos.ecall.automatic for a VEDS call placed due to a crash) or may be different for calls to an admin line, etc.

The "RequestUriCondition" object contains two members:

- "operator", which MUST be present and MUST be set to one of "EQ" (equals), "SS" (substring), or "NE" (not equal to). String comparisons are case-insensitive.
- "content", which MUST be present. This is the value to be compared with the call's Request-URI value using the test specified in "operator".

"RequestUriCondition" evaluates to 'true' if "operator" is "EQ" and the call's Request-URI exactly matches the value in "content" aside from case, or "operator" is "SS" and the call's Request-URI contains the value in "content" ignoring case, or "operator" is "NE" and the call's Request-URI does not exactly match the value in "content" ignoring case. Otherwise, it evaluates to 'false'.

3.3.3.1.14 Normal-NextHop Condition

"NormalNextHopCondition" tests the current value of the "Normal-NextHop" variable. The LoST Service URN Condition (Section 3.3.3.1.9) sets "Normal-NextHop" to the URI returned by the LoST query or marks it as undefined.

The "NormalNextHopCondition" object contains two members:

- "operator", which MUST exist and be set to one of "EQ" (equals), "SS" (substring), or "NE" (not equal to). String comparisons are case-insensitive.
- "content", which MUST exist. This value is compared against the current value of the NormalNextHop variable using the test specified by the "operator".

"Normal-NextHop" is undefined at the start of every call, and remains undefined until a LoST Service URN Condition (Section 3.3.3.1.9) succeeds. When undefined, it evaluates to an empty string.

© Copyright 2011-2022 National Emergency Number Association, Inc.

3.3.3.1.15 Incoming Queue Condition

"IncomingQueueCondition" tests the URI of the queue the call was received on.

The "IncomingQueueCondition" object contains two members:

- "operator" which MUST exist and be set to one of "EQ" (equals), "SS" (substring), or "NE" (not equal to). String comparisons are case-insensitive.
- "content" which MUST exist. This is the value to be compared with the queue URI using the test indicated by "operator".

3.3.3.1.16 SDP Offer Condition

This condition supports routing policy based on SDP offers. This allows construction of rules that route calls based on the media requested as well as the human interactive language of a media stream, as indicated in the SDP. SDP is used to negotiate media and optionally includes a list of human languages and directionality for each media line in the offer; the answer optionally contains a language per media line, typically a language from the media line in the offer.

The "SdpOfferCondition" object has multiple members, which test for various media and languages in the SDP offer, and evaluate to 'true' or 'false'.

The tests "video", "audio", "rtt", and "im" evaluate to 'true' if the message contains an SDP offer and the offer includes the corresponding media. In addition, "text" is equivalent to "rtt" or "im" (that is, true if either RTT or IM is offered). Within an "SdpOfferCondition" object, these tests are Boolean members that are set to 'true' to perform the test; they are omitted or set to 'false' to not perform the test. If the member is set to 'true', then the test evaluates to 'true' if the SIP INVITE contains an SDP offer and the offer includes the corresponding media, and evaluates to 'false' if the INVITE does not contain an SDP offer, or contains an SDP offer that does not include the corresponding media, or the call is a SIP MESSAGE (which does not contain SDP). If the member is set to 'false' or omitted, it is not evaluated.

Note that session mode instant messaging uses SDP, while pager mode does not.

SDP offers may include human interactive language attributes (RFC 8373) [173] containing language subtags listed in the IANA Registry [180]. In an SDP offer, each media offered may contain an 'hlang-send' and/or an 'hlang-recv' attribute. The 'hlang-send' attribute contains a list of one or more language(s) the offerer is willing to use when sending the media; 'hlang-recv' contains a list of one or more language(s) the offerer is willing to use when receiving the media. The list of languages is in preference order (first is most preferred). A media may be intended for interactive communication using a language in both directions or in one direction only.

© Copyright 2011-2022 National Emergency Number Association, Inc.

PSAPs can natively support more than one language (i.e., the PSAP may have bi- or multi-lingual call takers), and might be able to conference in external translation services for other languages. PSAPs natively support audio and text, and might natively support video or be able to conference in external relay services in cases in which a call requests video with sign language that did not originate via a relay service[17].

Communication with the caller is optimized when the caller's most-preferred language can be supported in each requested media. Using a caller's less-preferred language may hinder communication, but using an external translation service has its own set of non-optimal aspects.

Languages are indicated by their subtag entry in the IANA registry [180]. While languages may include multiple subtags (allowing specification of various aspects such as dialects and writing system), matching uses the subtags specified in the conditions tests, which optimally use just the major subtag (such as "en" for English). For example, a rule with a condition testing for "en" would match an offer indicating "en-US" (for English as generally used in the U.S.), "en-UK" (for English as generally used in the U.K.), and "en-CA" (for English as generally used in Canada), while a rule testing for "en-scotland" (for the Scottish dialect of English) would not match any of the three.

The "langAudio", "langText", "langVideo", "langRtt", and "langIm" members are arrays of strings; each array element contains one human interactive language (humintlang) (RFC 8373) [173] subtag. A member evaluates as 'true' if any of its language subtags matches one of the languages (for either direction) in the offer for the corresponding media (audio, text, video, RTT, IM). This allows the rule to ask, "Does the offer request audio using Spanish?" for example, and it will evaluate to 'true' if, in the example, the offer requests audio using Greek, Spanish, French, or German. These conditions allow creating language-specific queues and routing to the appropriate queue based on the humintlang (RFC 8373) [173] marking of the offer.

The "langAudioPref", "langTextPref", "langVideoPref", "langRttPref", and "langImPref" child objects test if a specific language is the most-preferred of the languages that match a set of languages offered for the corresponding media. Each of these objects contains two members: "langTest" is a string containing one language subtag; "langList" is an array of strings, each array element is a string containing one language subtag. The condition tests if the corresponding media (audio, text, video, RTT, IM) contains any of the "langList" languages (for either direction) and, if so, whether the "langTest" language is the most-preferred of the matching languages. This allows the rule to ask, "Is French the most-

[17] While calls requiring relay service normally originate via the service, a call might originate directly, (e.g., in the case of a visitor from a country in which calls are placed directly).

© Copyright 2011-2022 National Emergency Number Association, Inc.

preferred language of the set (English, French, Spanish) for audio in the offer?" It evaluates to true, in this example, if the offer specifies that Algonquian, French, and English (in that order) are available for an audio media stream. If, in contrast, the offer specified that English, Algonquian, and French (in that order) were available, the test would evaluate to false, since of the set (English, French, Spanish), English and French match, but of those, French is not the most-preferred. These conditions allow creating language-specific queues and routing to the appropriate queue based on the humintlang (RFC 8373) [173] marking of the offer, matching the most-preferred language of the caller with the languages natively supported at the PSAP.

The "SdpOfferCondition" object has the following members:

Boolean members: when set to 'true', evaluates as 'true' if the SDP contains the indicated media, and as 'false' if the SDP does not contain the indicated media:

- "video": for video media
- "audio": for audio media
- "rtt": for RTT
- "im": for IM
- "text": for either RTT or IM

The "video", "audio", "rtt", and "im" members MAY each occur; the "text" member MAY occur only if neither "rtt" nor "im" occurs.

String array members: each member is an array of strings, each element of which is a single language subtag; the member evaluates as 'true' if the SDP contains the indicated media using any of the languages in the array, and 'false' otherwise:

- "langVideo": for video
- "langAudio": for audio
- "langRtt": for RTT
- "langIm": for IM
- "langText": for either RTT or IM

Child objects: each MUST contain the following two members:

- "langList": array of strings, each element is a language subtag.
- "langTest": string containing a language subtag.

The child objects tests if the SDP includes the corresponding media using any of a set of languages of which the specified language is the most preferred:

- "langVideoPref": for video
- "langAudioPref": for audio
- "langRttPref": for RTT

© Copyright 2011-2022 National Emergency Number Association, Inc.

- "langImPref": for IM
- "langTextPref": for either RTT or IM

Each of the above "lang…Pref" child objects evaluates as 'true' if:

- the SDP includes the corresponding media, and
- the corresponding media uses any of the "langList" languages, and
- the "langTest" language tag is the most-preferred of the matching languages

Multiple members and/or child objects MAY occur in a single "SdpOfferCondition" object; they are interpreted with an implicit logical OR: if any evaluate to 'true', the condition evaluates to 'true'.

3.3.3.1.17 CAP Condition

CAP message parameters may be tested with the CAP Condition. (In addition to the tests in this condition, which test for certain specific CAP elements, any CAP element can also be tested using the more general Body Part Condition described in Section 3.3.3.1.12).

The following child objects are defined for use within a "CapCondition" object:

- "Identifier",
- "Sender",
- "Address",
- "InfoEventCode",
- "InfoValueName".

Each of these child objects contains two members:

- "operator", which MUST exist and be set to one of "EQ" (equals), "SS" (substring), or "NE" (not equal to). String comparisons are case-insensitive.
- "content", which MUST exist. This is the string that is compared with the corresponding element of the CAP component using the test indicated by "operator".

The above child objects are OPTIONAL, but at least one MUST occur. Multiple child objects MAY occur within a "CapCondition" object; they are interpreted with an implicit logical AND: if any evaluate to 'false, the condition evaluates to 'false.

The "CapCondition" object MAY contain the "NonInteractive" Boolean member. If this member exists and is set to 'true', it evaluates as 'true' if the CAP occurs in a non-Interative call (i.e., a SIP MESSAGE with CAP body), and as 'false' if the call is a SIP INVITE. If "NonInteractive" does not occur or is set to 'false', it has no effect on the evaluation of the "CapCondition" object. If "NonInteractive" evaluates to 'false' (i.e., it occurs and is set to 'true' but the CAP is in an INVITE), the "CapCondition" object evaluates to 'false' (even if all child objects evaluate to 'true').

© Copyright 2011-2022 National Emergency Number Association, Inc.

If the message does not contain a CAP body, or the CAP does not contain the indicated element, the "CapCondition" object evaluates to 'false'.

3.3.3.1.18 CallingNumberVerificationStatus condition

This condition allows testing the outcome of any validation of the calling number that may have been done by the Secure Telephone Identity Verification Service (STI-VS) FE.

The "CallingNumberVerificationStatusCondition" object has two members:

- "operator", which MUST exist and be set to either "EQ" or "NE"
- "value", which MUST exist and be set to an entry from the 3GPP 7.2A.20 "verstat" tel URI parameter definition (currently defined values "TN-Validation-Passed", "TN-Validation-Failed" and "No-TN-Validation")

The evaluation of this condition compares the result of calling number verification with the state contained in "value", using the test indicated by "operator".

If the call does not contain a "verstat" parameter, the call's verification status is considered to be "No-TN-Validation".

3.3.3.2 Actions

The conditions specified above are the "if" part of rules; the actions specified below are the "then" part. The actions within a rule determine which operations the ESRP performs in handling a call. Actions cause various operations to be executed. As described above, more than one rule might match; of the rules whose conditions match, the rule with the highest priority value is executed. Some actions do not directly affect the call (e.g., looking up a route, sending notifications, logging messages); other actions forward a call to its next point (the Route action), reject a call (the Busy action), or switch control to a different rule set (the Invoke Policy action, which then evaluates that set of rules). Rules MUST NOT contain more than one Route, Busy or Invoke Policy action, or a combination of Route, Busy or Invoke Policy actions.

"Actions" is an array of action objects, as described below. An action object contains the following members:

- actionType: a string which MUST exist and be set to the specific action type.
- "description": an OPTIONAL string containing a description of the action.
- Other action-specific members as described in the below subsections.

© Copyright 2011-2022 National Emergency Number Association, Inc.

3.3.3.2.1 Route Action

This action forwards the call (as its SIP message) to a specific URL. If the final response to this forwarded INVITE/MESSAGE is not 200 OK, then the rule MUST be treated as if it evaluated to 'false'.

The "routeAction" object has three members:

- "recipientUri", which MUST exist and contain a URI that will become the Route header field for the outgoing SIP message (the Request-URI is normally a service URN such as "urn:service:sos")
- "rnaTimer", which is OPTIONAL. This is the Ring No Answer timer; it is the time in seconds the ESRP will wait for a final response. If this member is omitted, the ESRP MUST use a provisioned value; a suggested default for the provisioned value is 20 seconds.
- "cause", which is OPTIONAL. This contains the value to be used within the Reason parameter of the topmost History-Info header field for the outgoing SIP message. The value MUST be an entry from the RouteCause Registry (Section 10.20)

The ESRP SHALL implement a Ring No Answer timer, which SHALL be set to the "rnaTimer" value if present, or the provisioned default if omitted. If the timer expires before the final response to the forwarded SIP message is received, the Route action fails and is treated as if the rule condition evaluated to 'false' (i.e., the rule set is reevaluated and the highest priority rule whose conditions evaluated to 'true' is executed).

A Route Action can fail for reasons other than Ring No Answer timeout (e.g., because the destination queue becomes unreachable, the next hop rejected the call with an error status, or the call times-out before it is answered). In such cases, the ESRP MUST set its queue state for the target queue to "Unreachable" and MUST reevaluate the ruleset for the call. Note that its queue state remains "Unreachable" until a queue state notification resets it. The ESRP SHOULD set a minimum rate for queue state notifications to refresh state frequently.

When routing a call (as a result of a RouteAction or other reason), a RouteLogEvent is generated to note the route, and an optional text string "cause" stating why it chose the route.

3.3.3.2.2 Busy Action

The "BusyAction" object causes a final status of 600 Busy Everywhere to be sent toward the caller.

© Copyright 2011-2022 National Emergency Number Association, Inc.

3.3.3.2.3 Notify Action

This action sends a NOTIFY message to entities subscribing to the ESRP's "ESRPnotify" event package for the specified "eventCode". This may be used, for example, to advise other entities that calls are being diverted, etc.

The "NotifyAction" object has the following members:

- "recipient", which is OPTIONAL. When present, it MUST be either a URI or a service URN. This member is used to notify a single entity registered for the "eventCode". If "recipient" is a URI, notification is generated for that specific recipient. If "recipient" is a service URN, the ECRF is used to map the service URN to a URI, and a notification is generated for that URI. Recipients MUST have subscribed for the "eventCode" to get the notification. If "recipient" is omitted, notification is generated for all subscribers to the "eventCode". In all cases, notifications are subject to per-recipient throttling.
- "eventCode", which MUST exist and be set to a value contained in the EsrpNotifyEventCodes registry (Section 10.19).
- "urgency", which MUST exist and be set to an integer value from 0 and 100 where 0 is no urgency and 100 is the highest possible urgency.
- "comment", which is OPTIONAL. If present, it is a text string that is included in the "Comment" field of the NOTIFY message.

3.3.3.2.4 Log Message Action

This action causes a RouteRuleMsgLogEvent to be generated. This is primarily useful for debugging; implementations MAY provide a mechanism to switch logging of such messages on or off (i.e., when the mechanism is switched off, all occurrences of "LogAction" are ignored).

The "LogAction" object contains one member: "message", which is OPTIONAL.

The generated RouteRuleMsgLogEvent contains the policy owner, policy type, policy ID if policyType is "OtherRoutePolicy", policy queue name if policyType is "OriginationRoutePolicy" or "NormalNextHopRoutePolicy", rule ID, rule priority, and the contents of the "message" member if present.

3.3.3.2.5 Invoke Policy Action

Invoke Policy Action causes the specified policy routing ruleset to be evaluated. It is typically used to evaluate the policy ruleset associated with the URI received from a LoST query, allowing calls to be processed according to the policy of the next hop. This action

© Copyright 2011-2022 National Emergency Number Association, Inc.

may also be used to structure the routing rules of an entity as desired (e.g., into general and specific rulesets).

The "InvokePolicyAction" object has the following members:

- "policyType", which MUST exist and be set to one of the following subset of values from the Policy Types Registry Section 10.33:
  - OrginationRoutePolicy
  - NormalNexthopRoutePolicy
  - OtherRoutePolicy
- "policyId", which MUST exist when "policyType" is "OtherRoutePolicy" and MUST NOT exist otherwise.
- "policyQueueName"

The ESRP fetches a policy from the Policy Store using the specified "policyType", no owner, and a policyQueueName/policyId dependent on "policyType":

- For "OriginationRoutePolicy", policyQueueName is the queue the call arrived on and policyId is not used.
- For "NormalNexthopRoutePolicy", the policyQueueName is the value of the "Normal-NextHop" variable (as a result of a LostServiceUrnCondition evaluation as described in Section 3.3.3.1.9) and policyId is not used.
- For "OtherRoutePolicy", the policyId is the content of the "policyId" specified in the Invoke Policy Action and policyQueueName is not used.

If "Normal-NextHop" is undefined when an Invoke Policy action specifying "NormalNexthopRoutePolicy" is evaluated, or if the policy cannot be retrieved for any reason, the rule fails and is treated as if the rule condition evaluated to 'false'. "Normal-NextHop" is undefined if there is no Lost Service URN Condition in the rule, or the LoST query from the Lost Service URN Condition failed to result in a route.

3.3.3.3 PRR Ruleset Examples

```
{
    "description": "Call is probably spam.",
    "id":          "AA56i12",
    "priority":    7,

    "conditions":
    [
        {
            "conditionType": "CallSuspicionCondition",
            "scoreFrom": 70,
            "scoreTo":  100
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
            }
        ],

        "actions":
        [
            {
                "actionType": "RouteAction",
                "recipientUri":  "sip:special-treatment@psap.example.gov"
            }
        ]
    }


    {
        "description": "Rule for handling a SIP msg containing a CAP
    payload.",
        "id":          "AA56i11",
        "priority":    6,

        "conditions":
        [
            {
                "conditionType": "MimeBodyCondition",
                "mimeList": [ "application/common-alerting-protocol+xml" ]
            }
        ],

        "actions":
        [
            {
                "actionType":   "routeAction",
                "recipientUri": "sip:psap@home.example.gov"
            }
        ]
    }


    {
        "description": "Rule to consider time and queue state.",
        "id":          "AA56i10",
        "priority":    5,

        "conditions":
        [
            {
                "conditionType": "QueueStateCondition",
                "queue":         "sip:answering-machine@home.foo-bar.com",
                "condition":     "EQ",
                "value":         "Active"
            },
            {
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
            "conditionType": "TimePeriodCondition",
            "dateStart":     "19970105T083000",
            "timeStart":     "2200",
            "timeEnd":       "0800",
            "weekdayList":   "MO,TU,WE,TH,FR",
            "dateEnd":       "19991230T183000"
        }
    ],

    "actions":
    [
        {
            "actionType":   "routeAction",
            "recipientUri": "sip:answering-machine@home.foo-bar.com"
        }
    ]
}
```

The following example ruleset assumes a PSAP that natively supports voice and text, for both English and French. The ruleset checks if calls request a language and media supported natively; if so, calls are sent to specific queues for language and media; if not, calls are sent to a queue where an agent can authorize the use of third-party translation and/or relay services.

```
{
    "description": "
        ; ------------------------------------------------------
        ; If call requires language not supported natively,
        ; send to the translation approval queue:
        ; ------------------------------------------------------",

    "id":       "BB67m100",
    "priority": 100,

    "conditions":
    [
        {
            "negation":      true,
            "conditionType": "SdpOfferCondition",
            "langAudio":     "en",
            "langText":      "en",
            "langAudio":     "fr",
            "langText":      "fr"
        }
    ],

    "actions":
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
        [
            {
                "actionType":   "routeAction",
                "recipientUri": "sip:trans-approv@psap.example.gov"
            },
            {
                "actionType": "logAction",
                "message":    "Call requires language not natively supported"
            }
        ]
    }


    {
        "description": "
            ; ----------------------------------------
            ; If call receives translation approval, send to
            ; the Policy Routing Rules queue:
            ; ----------------------------------------",

        "id":       "AA56i222",
        "priority": 10,

        "conditions":
        [
            {
                "conditionType": "LostServiceUrnCondition",
                "urn":           "urn:emergency:service:sos.psap"
            }
        ],

        "actions":
        [
            {
                "actionType":   "InvokePolicyAction",
                "policyType":   "NormalNexthopRoutePolicy"
            }
        ]
    }


    {
        "description": "
            ; ----------------------------------------------------
            ; If call requires media not supported natively, it
            ; should have been initiated via a third-party relay
            ; service; since it wasn't, send to the special
            ; handling queue:
            ; ----------------------------------------------------",

        "id":       "BB67m090",
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
    "priority": 90,
    "negation": true,

    "conditions":
    [
        {
            "conditionType": "SdpOfferCondition",
            "audio":         true,
            "text":          true
        }
    ],

    "actions":
    [
        {
            "actionType":   "routeAction",
            "recipientUri": "sip:special-handling@psap.example.gov"
        },
        {
            "actionType": "logAction",
            "message":    "Call requires media not natively supported"
        }
    ]
}


{
    "description": "
        ; ----------------------------------------------------------
        ; If French is the most-preferred of (English, French),
        ; send to French queue
        ; ----------------------------------------------------------",

    "id":      "BB67m080",
    "priority": 80,

    "conditions":
    [
        {
            "conditionType": "SdpOfferCondition",
            "langAudioPref":
            {
                "langTest": "fr",
                "langList": [ "en", "fr" ]
            },
            "langTextPref":
            {
                "langTest": "fr",
                "langList": [ "en", "fr" ]
            }
        }
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
    ],

    "actions":
    [
        {
            "actionType":   "routeAction",
            "recipientUri": "sip:french@psap.example.gov"
        },
        {
            "actionType": "logAction",
            "message":    "French is most-preferred among English and
French"
        }
    ]
}


{
    "description": "
        ; ----------------------------------------------------------
        ; If English is the most-preferred of (English, French),
        ; send to English queue
        ; ----------------------------------------------------------",

    "id":       "BB67m070",
    "priority": 70,

    "conditions":
    [
        {
            "conditionType":   "SdpOfferCondition",
            "langAudioPref":
            {
                "langTest": "en",
                "langList": [ "en", "fr" ]
            },
            "langTextPref":
            {
                "langTest": "en",
                "langList": [ "en", "fr" ]
            }
        }
    ],

    "actions":
    [
        {
            "actionType":   "routeAction",
            "recipientUri": "sip:english@psap.example.gov"
        },
        {
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
            "actionType": "logAction",
            "message":    "English is most-preferred among English and
French"
        }
    ]
}


{
    "description": "
        ; ----------------------------------------------------------
        ; Can't-get-here rule that should never be executed.
        ;
        ; If this rule executes, we have an error, since the
        ; previous rules should have caught all cases. This rule
        ; has no <conditions> element, hence is considered
        ; to have a <conditions> that evaluates to true.
        ; ----------------------------------------------------------",

    "id":       "BB67m000",
    "priority": 0,

    "actions":
    [
        {
            "actionType":   "routeAction",
            "recipientUri": "special-handling@psap.example.gov"
        },
        {
            "actionType": "logAction",
            "message":    "ERROR: can't-get-here rule triggered"
        },
        {
            "actionType": "logAction",
            "message":    "====== File discrepancy report ======"
        }
    ]
}
```

To illustrate the effects of these rules, here are a few example SDP offers (only the most directly relevant portions of the SDP block are shown):
An offer requesting spoken Spanish both ways (most preferred), spoken Basque both ways (second preference), or spoken English both ways (third preference):

```
m=audio 49250 RTP/AVP 20
a=hlang-send:es eu en
a=hlang-recv:es eu en
```

In the immediately preceding ruleset:

© Copyright 2011-2022 National Emergency Number Association, Inc.

- The conditions of rule BB67m100 are 'false':
  - "langAudio" for "en" is 'true' (since audio is offered and "en" is one of the offered languages for audio);
  - "langText" for "en" is 'false' (since text is not offered)
  - "langAudio" for "fr" is 'false (since "fr" is not one of the offered languages for audio);
  - "langText" for "fr" is 'false' (since text is not offered)
  - the SDP Offer condition evaluates to 'true'
  - The "conditions" evaluation is reversed by the "negation" element;
- The conditions of rule AA56i222 are 'true' (assuming the LoST query succeeds);
- The conditions of rule BB67m090 are 'false':
  - "audio" is 'true' (since audio is offered)
  - "text" is 'false' (since text is not offered)
  - the SDP Offer condition evaluates to 'true'
  - The "conditions" evaluation is reversed by the "negation" element;
- The conditions of rule BB67m080 are 'false':
  - "langAudioPref" with "langTest" "fr", and "langList" "en" and "fr" evaluates to 'false' (since the offer for audio does not contain "fr");
  - "langTextPref" with "langTest" "fr", and "langList" "en" and "fr" evaluates to 'false' (since the offer does not contain text);
- The conditions of rule BB67m070 are 'true':
  - "langAudioPref" with "langTest" "en", and "langList" "en and "fr" evaluates to 'true' (since the offer requests "es eu en" in that order and the only offered language for audio in the set ("en", "fr") is "en", it is first (and only) in the matching set of "en");
  - "langTextPref" with "langTest" "fr", and "langList" "en fr" evaluates to 'false' (since the offer does not contain text);
- The conditions of rule BB67m000 are 'true', as the conditions are omitted;

So, three rules have conditions that evaluate to 'true':

- BB67m070: "priority" 70
- AA56i222: "priority" 10
- BB67m000: "priority" 0.

Since the highest (largest) priority matching value rule is executed, BB67m070 is executed, sending the call to the "sip:english@psap.example.gov" queue, and logging a message of "English is most-preferred among English and French".

An offer requesting written Greek both ways:

```
m=text 45020 RTP/AVP 103 104
a=hlang-send:gr
a=hlang-recv:gr
```

In the immediately preceding ruleset:

© Copyright 2011-2022 National Emergency Number Association, Inc.

- The conditions of rule BB67m100 are 'true':
  - "langAudio" for "en" is 'false (since audio is not offered);
  - "langText" for "en" is 'false' (since "en" is not one of the offered languages for text)
  - "langAudio" for "fr" is 'false' (since audio is not offered languages);
  - "langText" for "fr" is 'false' (since "fr" is not one of the offered languages for text)
  - the SDP Offer condition evaluates to 'false
  - The "conditions" evaluation is reversed by the "negation" element;
- The conditions of rule AA56i222 are 'true' (assuming the LoST query succeeds);
- The conditions of rule BB67m090 are 'false':
  - "audio" is 'false (since audio is not offered)
  - "text" is 'true (since text is offered)
  - the SDP Offer condition evaluates to 'true'
  - The "conditions" evaluation is reversed by the "negation" element;
- The conditions of rule BB67m080 are 'false':
  - "langAudioPref" with "langTest" "fr", and "langList" "en" and "fr" evaluates to 'false' (since audio is not offered);
  - "langTextPref" with "langTest" "fr", and "langList" "en" and "fr" evaluates to 'false' (since the text offer does not include "en" nor "fr");
- The conditions of rule BB67m070 are 'false:
  - "langAudioPref" with "langTest" "en", and "langList" "en and "fr" evaluates to 'false (since the offer does not include audio);
  - "langTextPref" with "langTest" "fr", and "langList" "en" and "fr" evaluates to 'false' (since the text offer does not include "en" nor "fr");
- The conditions of rule BB67m000 are 'true', as the conditions are omitted.

So, two rules have conditions that evaluate to 'true':

- BB67m100, "priority" 100
- AA56i222, "priority" 10
- BB67m000, "priority" 0.

Since the highest (largest) priority matching value rule is executed, BB67m100 is executed, sending the call to the "sip:trans-approv@psap.example.gov" queue, and logging a message of "Call requires language not natively supported".

An offer requesting spoken Cree both ways (most preferred), spoken English both ways (second preference), or spoken French both ways (third preference):

```
m=audio 49250 RTP/AVP 20
a=hlang-send:cr en fr
a=hlang-recv:cr en fr
```

In the immediately preceding ruleset:

- The conditions of rule BB67m100 are 'false':

© Copyright 2011-2022 National Emergency Number Association, Inc.

    - "langAudio" for "en" is 'true (since "en" is one of the offered languages for audio);
    - "langText" for "en" is 'false' (since text is not offered)
    - "langAudio" for "fr" is 'true (since "fr" is one of the offered languages for audio);
    - "langText" for "fr" is 'false' (since text is not offered)
    - the SDP Offer condition evaluates to 'true'
    - The "conditions" evaluation is reversed by the "negation" element;
- The conditions of rule AA56i222 are 'true' (assuming the LoST query succeeds);
- The conditions of rule BB67m090 are 'false':
    - "audio" is 'true' (since audio is offered)
    - "text" is 'false' (since text is not offered)
    - the SDP Offer condition evaluates to 'true'
    - The "conditions" evaluation is reversed by the "negation" element;
- The conditions of rule BB67m080 are 'false':
    - "langAudioPref" with "langTest" "fr", and "langList" "en" and "fr" evaluates to 'false' (since the offer for audio contains both "en" and "fr", but lists "fr" second among those two);
    - "langTextPref" with "langTest" "fr", and "langList" "en" and "fr" evaluates to 'false' (since the offer does not contain text);
- The conditions of rule BB67m070 are 'true:
    - "langAudioPref" with "langTest" "en", and "langList" "en and "fr" evaluates to 'true (since the offer requests "cr en fr" in that order, the offered language for audio in the set ("en", "fr") are both "en" and "fr", and "en" is first in the matching set of ("en", "fr");
    - "langTextPref" with "langTest" "fr", and "langList" "en fr" evaluates to 'false' (since the offer does not contain text);
- The conditions of rule BB67m000 are true, as the conditions are omitted;

So, three rules have conditions that evaluate to true:

- BB67m070: "priority" 70
- AA56i222: "priority" 10
- BB67m000: "priority" 0.

Since the highest (largest) priority matching value rule is executed, BB67m070 is executed, sending the call to the "sip:english@psap.example.gov" queue, and logging a message of, "English is most-preferred among English and French".

3.4 LoST

LoST (RFC 5222 [48]) is the protocol that is used for several functions:

© Copyright 2011-2022 National Emergency Number Association, Inc.

- Call routing: LoST is used by the ECRF as the protocol to route all emergency calls both to[18] and within the ESInet.
- Location validation: LoST is used by the LVF as the protocol to validate civic location information for every call origination end device prior to any potential use for emergency call routing.
- Retrieving URIs to support the retrieval of information based on a location such as Additional Data about that location and Agency Locator records.
- Retrieving lists of services available at a location.

The normative reference that defines the protocol is RFC 5222 [48], extended by draft-ecrit-lost-planned-changes [178]. The text in this section that defines LoST protocol operations should be considered informative, and any discrepancies are resolved by RFC 5222 text. The text below does contain limitations and specific application of LoST operations that are normative.

3.4.1 Emergency Call Routing using LoST

All SIP-based emergency calls pass location information either by value (PIDF-LO) or by reference (Location URI) plus a Service URN to an Emergency Service Routing Proxy (ESRP) to support routing of emergency calls. The ESRP passes the Service URN and location information[19] via the LoST interface to an Emergency Call Routing Function (ECRF), which determines the next hop in routing a call to the requested service. The ECRF performs the mapping of the call's location information and requested Service URN to, for example, a "PSAP URI" by querying its data and then returning the URI provided. Using the returned URI and other information (time of day, PSAP state, etc.), the ESRP then applies policy from a Policy-based Routing Function (PRF) to determine the appropriate routing URIs. This URI is the "next hop" in the call's routing path that could be an ESRP URI (intermediate hop), a PSAP URI (final hop), or even a call-taker (see Section 4.3 for a more detailed functional explanation of the i3 ECRF).

The service URN used to query the ECRF by an ESRP is obtained by provisioning of the "origination policy" of the queue that the call is received on at the ESRP (see Section 4.2.1.1). The response of the ECRF is determined by provisioning of the service boundary layers, which specify the URN they apply to (see Section 4.3.1). Thus, ECRFs (and ESRPs)

[18] LoST must be used within an ESInet to route calls. It is RECOMMENDED that originating networks also use LoST to route calls to the entry ESRP, but they MAY use appropriate local functions provided that calls are routed to the same ESRP as they would be if LoST were used to the authoritative ECRF.

[19] If an element using LoST receives location by reference, it MUST dereference the URI to obtain the value prior to querying the LoST server. The LoST server does not accept location by reference.

© Copyright 2011-2022 National Emergency Number Association, Inc.

are not hard-coded with any specific URNs, but the provisioning of the policy in the ESRP MUST match the provisioning of the service boundaries in the ECRF.

A single emergency call can be routed by one or more ESRPs within the ESInet, resulting in use of the LoST interface once per hop as well as once by the terminating PSAP.

Note that the term "PSAP URI" is used within the LoST protocol definition to refer to the URI returned from the service URN "urn:service:sos". In NG9-1-1, the URI returned may not be that of a PSAP, but instead may route to a BCF or ESRP.

3.4.2 Location Validation

Location validation is the validation of civic address-based location information against an authoritative GIS database containing only valid civic addresses obtained from 9-1-1 Authorities. Location validation is performed by the i3 LVF. "Validating" a location in NG9-1-1 means querying the Location Validation Function (Section 4.3) to determine if the location is suitable for use (specifically, if the location can be used to accurately route the call and dispatch responders). To be "LVF-Valid", thus "routable", a queried location using "urn:service:sos", or "urn:emergency:service:sos", or subservices of them MUST: 1) return a valid indication (i.e., no fields in the <invalid> list) from an LVF query with the location; and, 2) MUST yield a single <mapping> element in the LoST response. In general, this means the fields supplied in the LoST query match exactly one location (one address point in the site/structure layer, or a valid house number in a road segment layer).

We differentiate between the ECRF and LVF even though they have identical provisioning and identical interfaces because the ECRF query is made at call time while the LVF query is made during provisioning of a location in a LIS, and thus is non-real-time. LoST servers discovered using the 'LoST' service tag might refuse to perform location validation (e.g., when under stress). The 'LoST-Validation' service tag [224] provides a way to identify LoST servers designated to perform location validation.

The LVF MUST support the validation of location around planned changes as defined by draft-ecrit-lost-planned-changes [178].

3.4.3 <findService> Request

The "civic" and "geodetic-2d" profiles are baseline profiles defined in RFC 5222 [48]. Emergency calls are expected to use only these profiles. NG9-1-1 conformant LoST servers are NOT REQUIRED to support any location profiles beyond the baseline profiles defined in RFC 5222.

The ECRF/LVF SHOULD expect to receive any of the PIDF-LO elements described in the NENA Civic Location Data Exchange Format (CLDXF) [77] document within a civic location.

© Copyright 2011-2022 National Emergency Number Association, Inc.

The LoST interface allows a geo-location to be expressed as a point or one of a number of defined "shapes" such as circle, ellipse, arc-band, or polygon. ECRFs MUST be able to handle all of these shapes.

The "service" element identifies the service requested by the client. Valid service names MUST be "urn:service:sos" or one of its sub-services for ECRF and LVF queries used by originating networks or devices for emergency calls. For internal ECRFs used by entities within the ESInet to route calls, the <service> element MAY be a service URN beginning with "urn:emergency:service". ECRF implementations MUST support "urn:emergency:service". The use of such service URNs is dependent on provisioning of service boundary layers in the GIS. Service URNs are defined in Section 10.2.

The optional attribute to request validation occurs in a query and indicates whether location validation should be performed and is currently conditioned on the <location> element containing a civic address; (i.e., it is an error to request location validation for a geodetic coordinates-based location in RFC 5222). A request for validation MAY include elements defined in draft-ecrit-lost-planned-changes [178] to allow clients to validate locations against planned changes in the GIS data. Entities inside the ESInet MUST specify recursion by setting the recursive attribute in the <findService> request to 'true' and all ECRFs and LVFs MUST implement and perform recursion when requested to help mitigate the effect of an attack on the Internal Forest Guide (see Section 4.13.6). The internal ECRFs and LVFs (see Section 4.13), when they are under stress from attack, MAY refuse queries from entities they do not know. External queries MAY use either recursion or iteration, as the external Forest Guide will be publicly available.

3.4.4 <findService> Response

LoST servers MAY operate in recursive mode or iterative mode if the server being queried is not authoritative for the location supplied.

- The use of recursion by the ECRF or LVF initiates a query on behalf of the requestor that propagates through other ECRFs to an authoritative ECRF/LVF that returns the PSAP URI back through the intervening ECRFs to the requesting ECRF.
- The use of iteration by the ECRF/LVF simply returns a FQDN of the next ECRF to contact.

The ECRF MAY operate in a recursive mode or an iterative mode, depending on local provisioning and the value of the 'recursive' attribute of the <findService> request. All ECRF and LVF implementations MUST support both recursive and iterative modes. It is strongly RECOMMENDED that ECRFs and LVFs use recursion when the query allows it. This minimizes the time to complete a request, especially when ECRFs and LVFs make use of

© Copyright 2011-2022 National Emergency Number Association, Inc.

persistent TCP connections to parents and children within the common hierarchy of these services.

When the i3 ECRF successfully processes a LoST <findService> message, it returns a LoST <findServiceResponse> message containing a <mapping> element that includes the "next hop" ESRP or final PSAP URI in the <uri> element. If the ECRF cannot successfully process a LoST <findService> message, it returns a LoST <errors> message indicating the nature of the error or a LoST <redirect> message indicating the ECRF that can process the <findService> message.

The <uri> returned specifies either the next hop URI of the PSAP or the ESRP that is appropriate for the location sent in the query message. This MUST be a globally routable URI with a scheme of "sip" for "urn:service:sos". Some other service URNs MAY return values with HTTP/HTTPS schemes. For example, for the "urn:emergency:service:additionalData" service URN, LoST servers SHOULD return SIPS and HTTPS URIs in addition to the SIP and HTTP (when appropriate) URIs.

The 'expires' attribute in the <mapping> element provides an ECRF or LVF with a way to control load, balancing that against the time required to completely implement a routing change when circumstances require. By increasing the expiration time, fewer queries to the server may be received if upstream LoST servers or clients implement caching.

Adjusting the expiration time near the scheduled change time can better accommodate planned changes, especially for clients that do not implement [178].

Responses from ECRFs SHOULD have very short expiration times, typically measured in minutes or at most a few hours. This would allow routes to change quickly if failures resulted in an inability of the normal route to work. While this should be a very unlikely event, because other mechanisms to redirect calls without changing the URI retrieved from the LoST query should provide adequate backup, it may still happen when significant disasters occur and pre-planned backups are not available. It is NOT RECOMMENDED to return the "NO-EXPIRATION" value. The OPTIONAL "NO-CACHE" expires value may increase the load experienced by the ECRF and should be used only with due care.

The LoST response contains <via> elements in the <path> element that name the LoST servers visited to obtain the answer. Vias MUST be returned to be compliant with RFC 5222 and are essential for use in error resolution.

The <displayName> element of the <mapping> response is a text string that provides an indication of the serving agency(ies) for the location provided in the query. This information might be useful to PSAPs that query an ECRF. This capability could be used to provide English Language Translation (ELT)-type information that PSAPs receive from ALI databases today.

© Copyright 2011-2022 National Emergency Number Association, Inc.

The <service> element in the query identifies the service for which this mapping is valid. An ECRF outside the ESInet is REQUIRED to support the "urn:service:sos" service. Service substitution, as described in RFC 5222 [48], SHALL be used to substitute "urn:service:sos" for all subservices such as "urn:service:sos.police", which would cause the call to be routed the same as a call to "urn:service:sos". ECRFs inside the ESInet MUST support both "urn:service:sos" and "urn:emergency:service:sos". Support for other services will depend on local implementation. Routing of services inside the ESInet may depend on the (TLS) credentials of the client; routes for two services using the same service URN may receive different PSAP URIs. Note that if recursion is used, the credentials of the recursive server would be used, rather than the credentials of the original client.

The <serviceNumber> element in the <mapping> response contains the emergency services number appropriate for the location provided in the query. This allows a foreign end device to recognize a dialed emergency number. The service number returned by an ECRF or LVF for an emergency call MUST be "911".

A <mapping> element MAY contain a service boundary. See Section 4.3.3.3.

The <locationValidation> element in <findServiceResponse> identifies which elements of the received civic address were "valid" and used for mapping, which were "invalid", and which were "unchecked" when validation is requested. Since the ECRF is not responsible for performing validation, this parameter may not be returned, subject to local implementations. LVFs would always return <locationValidation> if <validateLocation> was set to "True" in the <findService> request.

To understand the validation portion of the response, follow these rules:

1. The combination of all elements appearing in the <valid> list defines the scope.
2. The combination of all elements appearing in the <invalid> list is not valid within the scope.
   a. No meaning can be inferred regarding the status of any individual element unless it is the only invalid element listed.
   b. The combination of elements may be valid in other scopes.
   c. One or more elements may appear as invalid even if they were not used in the original query, but could be used to resolve an ambiguity.
3. Any individual element appearing as unchecked (or used in the query but not appearing in any of lists) was not checked or could not be determined to be either valid or invalid.

If any element appears in the <invalid> list, the location information is invalid and SHOULD NOT be entered in the LIS unless, for example, there is no reasonable prospect of obtaining better information before an emergency call could be placed, or the location is

© Copyright 2011-2022 National Emergency Number Association, Inc.

believed correct (and thus the ECRF data is believed incorrect, and a discrepancy report has been filed).

Provisioning of the LoST server is defined by Section 3.6 and Appendix B. Two of the "layers" provisioned in the servers are the Centerline and Site/Structure layers. The former describes segments of a road, and may include address ranges. The latter describes a single addressable location and has a single address number. If both are provisioned, with the range overlapping the address points, any PIDF-LO containing a number in the range will be accepted as valid (address number not in the invalid list) regardless of which address points are present.

3.4.5 locationInvalidated

A LoST server operating as an LVF MUST support draft-ecrit-lost-planned-changes [178]. If it receives a URI for a location from a client, the LVF server MUST execute an HTTPS POST containing the <locationInvalidated> object against that URI when a change in GIS data will make that record invalid at a known future date. The "AsOf" attribute of the <locationInvalidated> object SHOULD be set to the date and time the GIS data will make the proffered location invalid. Note that if "AsOf" is used, expired and effective dates must be present in the data.

3.4.6 getServiceBoundary

If a LoST server returns a service boundary by reference, it MUST handle getServiceBoundary requests.

3.4.7 listServices and listServicesByLocation

All ECRFs and LVFs MUST implement listServices and listServicesByLocation. The response to this request may depend on the (TLS) credentials of the querier. A query with no <service> element in the request SHOULD result in "urn:service:sos" and possibly "urn:emergency:service" (the top level services) being returned in the response. A query with <service> specified as "urn:service:sos" SHOULD result in all the subservices of sos (sos.police, sos.fire, …) that are available in the jurisdiction being returned in the response. Entities inside the ESInet MUST specify recursion by setting the recursive attribute in the <listServicesByLocation> request to true.

3.4.8 Error Responses

- <badRequest> Element
  This element indicates the ECRF/LVF could not parse or otherwise understand the request sent by the requesting entity (e.g., the XML is malformed).

© Copyright 2011-2022 National Emergency Number Association, Inc.

- <forbidden> Element
  This element indicates an ECRF/LVF refused to send an answer. This generally only occurs for recursive queries, namely, if the client tried to contact the authoritative server and was refused.
- <internalError> Element
  This element indicates the ECRF/LVF could not satisfy a request due to a bad configuration or some other operational and non-LoST protocol-related reason.
- <locationProfileUnrecognized> Element
  None of the profiles in the request were recognized by the server.
- <locationInvalid> Element
  This element indicates the ECRF/LVF determined the geodetic or civic location is invalid (e.g., geodetic latitude or longitude value is outside the acceptable range). The only time this would normally be returned is if there was a malformed location such as profile="geodetic-2d" and <civicAddress> element present. If there is no authoritative server for the location, that would be coded as "notFound".
- <SRSInvalid> Element
  This element indicates the ECRF/LVF does not recognize the spatial reference system (SRS) specified in the <location> element or it does not match the SRS specified in the profile attribute (e.g., not WGS84 2D, EPSG Code 4326 for profile="geodetic-2d"). Note that this error is not present in the RFC 5222 schema, has been reported as an errata, and thus may not be implemented by all LoST servers or clients. Use of this error may be problematic.
- <loop> Element
  During a recursive query, the server was about to visit a server that was already in the server list in the <path> element indicating a request loop.
- <notFound> Element
  The ECRF/LVF cannot find an answer to the query. This occurs if the authoritative server cannot find the location and has no applicable default mapping, or if no authoritative server exists.
- <serverError> Element
  An answer was received from another LoST server, but it could not be parsed or otherwise understood. This error occurs only for recursive queries.
- <serverTimeout> Element
  This element indicates the ECRF timed out waiting for a response (e.g., another ECRF for a recursive query, etc.).
- <serviceNotImplemented> Element
  This element indicates the ECRF detected the requested service URN is not implemented and it found no substitute for it. This normally would not occur for a service beginning "urn:service:sos" unless 9-1-1 service is not available in that area.

© Copyright 2011-2022 National Emergency Number Association, Inc.

3.4.9 Warnings

A LoST response MAY contain one or more of the following warnings. Each warning comes with a "message" attribute with content in a human-readable format.

- locationValidationUnavailable
  A LoST server MAY return this element in the response to indicate it cannot fulfill a validation request.
- serviceSubstitution
  A LoST server MAY return this element in the response to indicate that it cannot fulfill a <findService> request for the service URN specified.
- defaultMappingReturned
  A LoST server MAY return this element in the response to indicate it cannot fulfill a <findService> request for the specified location but is able to respond with a default URI.
- uriNotStored
  A LoST server operating as an LVF supporting draft-ecrit-lost-planned-changes [178] MUST return this element in the response if the URI provided by the LoST client in the <plannedChange> element was not stored.

3.4.10 LoST Extensions

The standard information returned within the <locationValidation> element of a LoST <findServiceResponse> is somewhat limited. In order to aid a consumer of the response in assessing the quality and validity of the queried location, it may be helpful to indicate what type of match was used by the LVF's geocoding logic. It may also be helpful if the LVF can explicitly warn when such a match is of lesser quality than might be expected. Therefore, two extensions to LoST are defined for this purpose. The first is an element to indicate the type of match used, and is placed at the existing extension point of the <locationValidation> element. The second is a new warning element which can be used at the existing extension point within the standard <warnings> element of the response.

3.4.10.1 matchType Element

The <matchType> element is intended to contain an indication of the type of data used by the LVF's geocoding logic when attempting to match the location supplied in the request to the GIS data that has been provisioned. The value of the element is an xsd:token, and must be a registered value. It is RECOMMENDED that ECRFs and LVFs implement match type. If more than one token would apply, then "Hybrid" is used. A registry for <matchType> tokens is defined in Section 10.31.

© Copyright 2011-2022 National Emergency Number Association, Inc.

3.4.10.1.1 XML Schema Definition

The <matchType> element is placed at the extension point defined with the <locationValidation> element of a LoST <findServiceResponse> and is defined by the following schema:

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs=http://www.w3.org/2001/XMLSchema
 elementFormDefault="qualified"
 targetNamespace="urn:emergency:xml:ns:lostExt:validation1"
 xmlns:ns1="urn:emergency:xml:ns:lostExt:validation1">
   <xs:element name="matchType" type="xs:token"/>
</xs:schema>
```

This capability MAY be provided by an ECRF/LVF.

3.4.10.2 degradedMatch Element

The <degradedMatch> warning reuses the BasicException pattern from LoST and is placed at the extension point defined in the exceptionContainer of a findServiceResponse. The warning may include an optional message containing human-readable text. The warning is intended to convey the notion that the location queried was not able to be matched using the best available data. An example of this is when a location does not match any provisioned address points, but still falls within a range of addresses associated with a road centerline. The determination of "best available data" is left to the discretion of the LVF, and may vary from one geographic region to another. It is RECOMMENDED that ECRFs and LVFs implement degradedMatch. An LVF SHOULD NOT return a degradedMatch warning if there is no potential for improvement (e.g., a road centerline match in a region where address points are not able to be provisioned).

3.4.10.2.1 XML Schema Definition

The degraded match warning is defined by the following RelaxNG schema:

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs=http://www.w3.org/2001/XMLSchema
 elementFormDefault="qualified"
 targetNamespace="urn:emergency:xml:ns:lostExt:validation1"
 xmlns:ns1="urn:emergency:xml:ns:lostExt:validation1">
   <xs:element name="matchType" type="xs:token"/>
</xs:schema>
```

This capability MAY be provided by an ECRF/LVF.

3.4.10.3 Example

The following example shows both the <matchType> element and the <degradedMatch> warning.

© Copyright 2011-2022 National Emergency Number Association, Inc.

```
<findServiceResponse xmlns="urn:ietf:params:xml:ns:lost1">
  <mapping expires="2016-10-28T12:44:30Z" lastUpdated="2015-06-
22T18:05:17Z" source="lost.example.com" sourceId="7608">
    <displayName xml:lang="en">Police Dispatch</displayName>
    <service>urn:service:sos</service>
    <uri>sip:sos@psap.example.com</uri>
    <serviceNumber>911</serviceNumber>
  </mapping>
  <locationValidation
    xmlns:ca="urn:ietf:params:xml:ns:pidf:geopriv10:civicAddr"
    xmlns:lv1="urn:emergency:xml:ns:lostExt:validation1">
    <valid>ca:country ca:A1 ca:A3 ca:RD ca:STS</valid>
    <invalid />
    <unchecked>ca:HNO</unchecked>
    <lv1:matchType>RoadCenterline</lv1:matchType>
  </locationValidation>
  <warnings source="lost.example.com">
    <degradedMatch xmlns="urn:emergency:xml:ns:lostExt:degraded"
message="The location was matched using road centerlines." xml:lang="en"
/>
  </warnings>
  <path>
    <via source="lost.example.com" />
  </path>
  <locationUsed id="nsTrQMffoEa74" />
</findServiceResponse>
```

3.4.10.4 Call and Incident ID Extension to LoST

This document defines an extension to LoST, which adds Call Identifiers and Incident Tracking Identifiers to any LoST request. All elements that implement LoST MUST implement the Call and Incident ID extension.

3.4.10.4.1 XML Schema Definition

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
elementFormDefault="qualified"
targetNamespace="urn:emergency:xml:ns:lostExt:Ids"
xmlns:ns1="urn:emergency:xml:ns:lostExt:Ids">
  <xs:element name="emergencyCallIncidentId">
    <xs:complexType>
      <xs:attribute name="callId" use="required" type="xs:token"/>
      <xs:attribute name="incidentTrackingId" use="required"
       type="xs:token"/>
    </xs:complexType>
  </xs:element>
</xs:schema>
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

3.4.10.5 Too Many Mappings Warning Extension to LoST

This document defines an extension to LoST, which adds a Too Many Mappings warning to a <findServiceResponse>. It is RECOMMENDED that ECRFs and LVFs implement TooManyMappings.

3.4.10.5.1 XML Schema Definition

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
 targetNamespace="urn:emergency:xml:ns:lostExt"
 xmlns:lost="urn:ietf:params:xml:ns:lost1"
 elementFormDefault="qualified">
   <xs:import namespace="urn:ietf:params:xml:ns:lost1"
    schemaLocation="lost1.xsd"/>
   <xs:element name="tooManyMappings" type="lost:basicException"/>
</xs:schema>
```

3.4.11 LoST Query Examples

3.4.11.1 Civic Address-based Call Routing LoST Interface Example Scenario

A <findService> well-formed civic address query:

```
<?xml version="1.0" encoding="UTF-8"?>
  <findService xmlns="urn:ietf:params:xml:ns:lost1"
    recursive="true" serviceBoundary="value">
    <location id="627b8bf819d0bcd4d" profile="civic">
      <civicAddress
        xmlns="urn:ietf:params:xml:ns:pidf:geopriv10:civicAddr">
        <country>US</country>
        <A1>OH</A1>
        <A3>Columbus</A3>
        <RD>Airport</RD>
        <STS>Drive</STS>
        <HNO>2901</HNO>
        <NAM>Courtyard Marriott</NAM>
        <PC>43219</PC>
        <Room>Board Room B</Room>
      </civicAddress>
    </location>
    <service>urn:service:sos</service>
  </findService>
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

A <findServiceResponse> response to a well-formed query:

```
<?xml version="1.0" encoding="UTF-8"?>
    <findServiceResponse xmlns="urn:ietf:params:xml:ns:lost1">
      <mapping
        expires="2010-01-01T01:44:33Z"
        lastUpdated="2009-09-01T01:00:00Z"
        source="esrp.state.oh.us.example"
        sourceId="e8b05a41d8d1415b80f2cdbb96ccf109">
        <displayName xml:lang="en">
          Columbus PSAP
        </displayName>
        <service>urn:service:sos</service>
        <serviceBoundary
          profile="civic">
          <civicAddress
            xmlns="urn:ietf:params:xml:ns:pidf:geopriv10:civicAddr">
            <country>US</country>
            <A1>OH</A1>
            <A3>Columbus</A3>
          </civicAddress>
        </serviceBoundary>
        <uri>sip:columbus.psap@state.oh.us</uri>
        <serviceNumber>911</serviceNumber>
      </mapping>
      <path>
        <via source="ecrf.state.oh.us"/>
      </path>
      <locationUsed id="627b8bf819d0bcd4d"/>
    </findServiceResponse>
```

A <findService> civic address query with partial information:

```
<?xml version="1.0" encoding="UTF-8"?>
   <findService xmlns="urn:ietf:params:xml:ns:lost1"
     recursive="true" serviceBoundary="value">
     <location id="627b8bf819d0bcd4d" profile="civic">
       <civicAddress
         xmlns="urn:ietf:params:xml:ns:pidf:geopriv10:civicAddr">
         <country>US</country>
         <A3>Columbus</A3>
         <RD>Airport</RD>
         <STS>DR</STS>
         <HNO>2901</HNO>
         </civicAddress>
     </location>
     <service>urn:service:sos</service>
   </findService>
```

An <error> response to a partially-formed query:

```
<?xml version="1.0" encoding="UTF-8"?>
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
<errors xmlns="urn:ietf:params:xml:ns:lost1"
  source="ecrf.state.oh.us">
   <badRequest message="invalid XML fragment" xml:lang="en"/>
</errors>
```

This response scenario indicates an error that the server cannot find an answer to the query.

Note: Further examples of call routing will be provided in a future version of this document.

3.5 Event Notification

Events are communicated within and between ESInets using the SIP SUBSCRIBE/NOTIFY mechanism described in RFC 6665 [14]. ESInet functional elements MAY need to accept or generate events to outside elements using different asynchronous event notification mechanisms, which MUST be interworked to SIP SUBSCRIBE/NOTIFY at the ESInet boundary.

NG9-1-1 events are defined by an event package which includes the name of the event, the subscription parameters, the conditions under which NOTIFYs are issued and the content of the NOTIFY, as described in RFC 6665.

3.6 Spatial Interface for Layer Replication

Geospatial data is stored in a Geographic Information System (GIS). This document does not standardize the GIS. However, the data in the GIS is used to provision the ECRF, the LVF, the Mapping Data Service, and other functions. In order to provide a standardized interface from the GIS to the rest of the functional elements that need GIS data, this document describes a "Spatial Interface" (SI), which is a standardized interface towards data consumers such as the ECRF/LVF.

The SI could be built into a GIS system, or could be a stand-alone element with proprietary interfaces to GIS systems and the standardized interface towards the data consumers. The data model provided by the SI is based on the conventional GIS layer that consists of a set of geospatial features, each of which could be a point, line, or polygon, or a set of points, lines, or polygons. Each feature has a set of named attributes. For example, a part of a road might be represented as a set of connected straight lines of the road centerline, with attributes that name the road and provide the range of address numbers in that segment of the road.

An SI provides an interface between an authoritative copy of GIS data and functional elements within an ESInet such as an ECRF and LVF. An SI layer replication interface is used within the ESInet to maintain copies of the data in the layers of the authoritative GIS system that drives routing and display of maps throughout the system. Furthermore, any

© Copyright 2011-2022 National Emergency Number Association, Inc.

element that obtains GIS data via the SI could provide copies of the data to another element with the same interface, thus permitting wide distribution of authoritative data. The SI interface is near-real-time: an authorized change to the authoritative GIS will be reflected in the copies nearly immediately via the SI.

The SI MUST implement the server side of the ElementState event notification package and permit any ECRF or LVF that receives a feed from it to subscribe to it.

The data structure for the SI is defined in Appendix B. The GIS Data Model [184] need not be the same as that defined for the SI: the SI could transform internal GIS data to the SI structure.

OGC Document OGC 10-069r2 [94] describes a layer replication interface service for geospatial databases using the Web Feature Service (WFS) [93] and the ATOM protocol (RFC 4287 [95] and RFC 5023 [96]). Essentially, the changes in the database are expressed in WFS Insert/Update/Delete actions and ATOM is used to move the edits from the master to the copy. GeoRSS (http://www.georss.org) is a very simple mechanism used to encode the GML in RSS feeds for use with ATOM. There are three ATOM feeds proposed by OGC 10-069r2; a change feed, a resolution feed, and a replication feed. The SI layer replication interface is patterned after the replication feed described within OGC 10-069r2.

3.7 Discrepancy Reporting

Errors and discrepancies may occur in any set of data, including databases, configurations, etc. The functional elements described in this document MUST support the discrepancy report (DR) function. The DR function allows any entity to notify agencies and services (including the BCF, ESRP, ECRF, Policy Store, and LVF) when any discrepancy is found. The discrepancy report function is intended to be generated by any entity that is using the data and finds a problem. DRs are not intended to be an alarm function requiring immediate response. Examples include:

- The LIS might need to file a Discrepancy Report on the LVF.
- The ECRF/LVF may be receiving data from another ECRF/LVF and thus might need to file a DR on its upstream provider.
- The ECRF/LVF might need to file a DR on the GIS.
- The ESRP might need to file a DR on the owner of a routing policy (PSAP, ESRP) that has a problem.
- The PSAP might need to file a DR on an ESRP if a call is misrouted.
- The PSAP might need to file a DR on the GIS when issues are found in a map display.
- Any client of an ECRF might need to file a DR on the routing data (which could be a GIS layer problem or something else).

© Copyright 2011-2022 National Emergency Number Association, Inc.

- A PSAP or ESRP might need to file a DR on a LIS.
- A PSAP or ESRP might need to file a DR on an ADR/IS-ADR.
- A BCF, ESRP, or PSAP needs to file a DR on an originating network sending it a malformed call.
- Any client might need to file a DR on the ESInet operator (e.g., for general networking issues such as high latency, packet loss, incorrect DNS, or DHCP behavior).
- One PSAP might need to file a DR on another PSAP that transferred a call to it
- A data user might need to file a DR on a data owner due to rights management issues.
- A log client (logging entry or query) might need to file a DR on the Logging Service
- Any entity might need to file a DR on another entity due to authentication issues (bad certificate, unknown entity, etc.).
- An ESRP or PSAP might need to file a DR on a Border Control Function
- Any Policy Enforcement Point might need to file a DR on a Policy owner due to formatting, syntax or other errors in the policy.
- A Test Call Generator might need to file a DR on a PSAP for problems encountered when generating a test call.
- An entity verifying signed LogEvents might need to file a DR against an entity that logged an event if it is unable to obtain the certificate or verify the signature.

This document provides a standardized Discrepancy Reporting mechanism in the form of a web service. Each database, service, and agency MUST provide a Discrepancy Reporting web service. When a discrepancy is reported on an element (such as an ECRF), the DR is reported using a DR web service operated by the entity that operates the element, not necessarily by the element itself. While an automated mechanism is specified to handle sending and receiving of DRs and the responses to those DRs, humans will usually be responsible for generating and acting on them. Since a human will be involved, there might be noticeable time elapsed from the sending of the report to receiving the resolution; a call-back mechanism is provided for the responding agency to send the resolution to the reporting agency.

A Discrepancy Report (DR) is submitted by the entity reporting the discrepancy to a responding entity and passes through several phases:

- The reporting entity creates the DR and submits it to the responding entity.
- The responding entity acknowledges the DR and provides an estimate of when it will be resolved.
- The reporting entity may request a status update and receive a response.
- The responding entity resolves the DR and reports its resolution to the reporting entity using the call-back mechanism.

© Copyright 2011-2022 National Emergency Number Association, Inc.

All DRs MUST contain common data elements (a prolog) that include:

- Time Stamp of Discrepancy Submittal
- Discrepancy Report ID (a unique value generated by the reporting entity)
- Discrepancy reporting entity FQDN
- Discrepancy reporting agent user ID
- Discrepancy reporting contact info
- Service or Instance in which the discrepancy exists
- Discrepancy Report type (from the list of DRs in this section)
- Additional notes/comments
- Reporting entity's assessment of severity
- Discrepancy Service or Database specifics (as specified in the specific DR in this section)

For each type of Discrepancy Report there is a specific database or service where the discrepancy originated or occurred, and a defined block of data specific to the Discrepancy Report type. This DR-specific block includes:

- Query that generated the discrepancy
- Full response to the query that generated the discrepancy (Message ID, Result Code, etc.)
- What the reporting entity thinks is wrong
- What the reporting entity thinks is the correct response, if available

FEs creating Discrepancy Reports SHOULD limit the rate of similar reports to avoid having the DR service become a denial of service attack.

The Service/Agency Locator (Section 4.15) provides the URI to an agency or service's DR interface.

3.7.1 Discrepancy Report

The Discrepancy Reporting web service is used by a reporting entity to initiate a Discrepancy Report. The OpenAPI description of this web service can be found in Appendix E.2. It supports the following functions:

HTTP method: POST

Resource name .../Reports

Submits a Discrepancy Report. The DR is in the body of the POST, consisting of:

Name	Condition	Description
resolutionUri	MANDATORY	URI for responding entity to use for responses
reportType	MANDATORY	Type of DR (enumeration)

© Copyright 2011-2022 National Emergency Number Association, Inc.

Name	Condition	Description
discrepancyReportSubmittalTimeStamp	MANDATORY	Timestamp of Discrepancy Report Submittal
discrepancyReportId	MANDATORY	Unique (to reporting agency) ID of report
reportingAgencyName	MANDATORY	FQDN of the entity creating the report
reportingAgentId	OPTIONAL	UserId of agent creating the report
reportingContactJcard	MANDATORY	jCard of contact about this report
problemService	Conditional, MUST be provided for specified DRs	Name of service or instance where discrepancy exists
problemSeverity	MANDATORY	One of the following tokens representing the reporting entity's opinion of the discrepancy's severity: • Minor (e.g., format/spelling) • Moderate (still functions) • Degraded • Impaired • Severe (service down but calls can proceed) • Critical (calls impaired)
problemComments	Conditional, MUST be provided for specified DRs, OPTIONAL otherwise	Text comment

The object has additional "reportType"-dependent parameters, listed in subsections below. Each database/service-specific discrepancy report description indicates whether the "problemService" and/or "problemComments" parameter is required for that database/service or not, and specifies additional parameters contained in the submitted object.

The resolution to the Discrepancy Report is sent to the URI in the resolutionUri parameter of the request.

© Copyright 2011-2022 National Emergency Number Association, Inc.

A successful report submission returns a DiscrepancyReportResponse that consists of:

Name	Condition	Description
respondingAgencyName	MANDATORY	FQDN of agency responding to report
respondingContactJcard	MANDATORY	jCard of contact about this response
respondingAgentId	OPTIONAL	UserId of agent creating the response report
responseEstimatedReturnTime	OPTIONAL	Estimated response time stamp
responseComments	OPTIONAL	Text comment

Status Codes

201 Report successfully created
454 Unspecified Error
470 Unknown Service/Database ("not ours")
471 Unauthorized Reporter

3.7.2 Discrepancy Resolution

When the responding agency determines what the resolution to the DR is, it sends the resolution to the ResolutionUri parameter in the report request.

HTTP method: POST

Resource name …/Resolutions

The POST contains a DiscrepancyResolution in the body, consisting of:

Name	Condition	Description
respondingAgencyName	MANDATORY	FQDN of entity responding to the report
respondingContactJcard	MANDATORY	jCard of contact about this report
respondingAgentId	OPTIONAL	UserId of agent responding to the report
discrepancyReportId	MANDATORY	Unique (to reporting agency) ID of report
reportingAgencyName	MANDATORY	FQDN of agency creating the report
problemService	MANDATORY	Name of service or instance where discrepancy exists
responseTime	MANDATORY	Time stamp of response

© Copyright 2011-2022 National Emergency Number Association, Inc.

Name	Condition	Description
responseComments	OPTIONAL	Text comment
resolution	MANDATORY	Details how the DR was resolved, as described in the DR-specific resolutions in the following subsections

Status Codes

201	Discrepancy Resolution successfully created
454	Unspecified Error
472	Unauthorized Responder
473	Unknown ReportId

The report can be retrieved based on the Agency Name and discrepancyReportId

HTTP method: GET

Resource name .../Resolutions

Name	Condition	Description
agencyName	MANDATORY	FQDN of entity reporting the discrepancy
discrepancyReportId	MANDATORY	Id of the report

A successful response returns the DiscrepancyResolution object described above

Status Codes

200	Resolution found
404	Not Found
471	Unauthorized Reporter
473	Unknown ReportId
475	Response not available yet

3.7.3 Status Update

A reporting entity MAY request a status update. The mechanism defined assumes the responding entity continuously tracks the status of Discrepancy Reports that it has received (including those it has recently resolved), and can respond to the Status Update immediately. The update request includes:

HTTP method: GET

Resource name .../StatusUpdates

© Copyright 2011-2022 National Emergency Number Association, Inc.

Name	Condition	Description
reportingAgencyName	MANDATORY	FQDN of entity that created the original report
discrepancyReportId	MANDATORY	Unique (to reporting agency) ID of original report

A successful response to this request includes a StatusUpdate object consisting of:

Name	Condition	Description
respondingAgencyName	MANDATORY	FQDN of the entity responding to the report
RespondingContactJcard	MANDATORY	jCard of contact about this report
respondingAgentId	OPTIONAL	UserId of agent responding to the report
responseEstimatedReturnTime	MANDATORY	Estimated date/time when response will be returned to reporting agency or the actual time, in the past, when the response was provided.
statusComments	OPTIONAL	Text Comment

Status Codes

200	OK
404	Not Found
454	Unspecified Error
471	Unauthorized Reporter
454	Unspecified Error
471	Unauthorized Reporter
473	Unknown ReportId
474	Resolution already provided

3.7.4 Policy Store Discrepancy Report

A client of a Policy Store MAY report a discrepancy. The most commonly expected report is that a Policy Query returned an invalid Policy from the Policy Store. A Policy Owner MAY retrieve a policy it previously stored to verify that the returned policy is valid and an exact match of that stored, and if not, file a discrepancy report against the Policy Store. A Policy Store MAY report a discrepancy against itself to raise an issue to be addressed.

© Copyright 2011-2022 National Emergency Number Association, Inc.

When a **PolicyStoreDiscrepancyReport** is submitted, the "problemService" parameter is set to "PolicyStore" and the object contains the following elements:

Name	Condition	Description
policyType	CONDITIONAL, at least one of policyType, policyOwner, policyId or policyQueueName MUST be provided	Type of the policy. Values are limited to names in the Policy Types registry
policyId	CONDITIONAL, MUST NOT be specified unless policyType is "OtherRoutePolicy"	For "OtherRoutePolicy", this is an arbitrary identifier for the policy
policyQueueName	CONDITIONAL, MUST NOT be specified unless policyType is "OriginationRoutePolicy" or "NormalNextHopRoutePolicy"	For "OriginationRoutePolicy" or "NormalNextHopRoutePolicy", this is the policyQueueName
policyAgencyName	MANDATORY	The agency whose policy is requested. Must be a FQDN or URI that contains a FQDN
problem	MANDATORY	One of the following tokens: • PolicyInvalid • PolicyAltered • SignatureVerificationFailure • PolicyMissing • OtherPolicyStore
retrievePolicyResponse	MANDATORY	The Response received from the Policy Retrieve Request as shown in Section 3.3.1

The Resolution parameter in a Policy Store Discrepancy Resolution report contains one of the following tokens:

- PolicyAdded
- PolicyUpdated
- NoSuchPolicy
- InsufficientCredentials
- NoDiscrepancy

© Copyright 2011-2022 National Emergency Number Association, Inc.

- OtherResponse

3.7.5 LoST Discrepancy Report

A client of an LVF/ECRF/LoST server (see Section 3.4) MAY report a discrepancy. An ECRF/LVF MAY report a discrepancy against another ECRF/LVF from which it receives data. An ECRF/LVF MAY report a discrepancy against itself to raise an issue to be addressed. The expected reports are:

- the LoST server reports a location as invalid, when the client believes it is valid;
- a LIS MAY report a discrepancy against an LVF (as well as against an Originating Service Provider) if a civic address provisioned by an Originating Service Provider for a fixed device is reported invalid by an LVF;
- the LoST server returned an incorrect route in a findServiceResponse;
- the LoST server returned an incorrect error or warning regarding the location;
- the getServiceBoundaryResponse is incorrect;
- the listServicesResponse is incorrect;
- the listServicesByLocationResponse is incorrect.

Other discrepancies may be reported but are expected to be less common. These include:

- a client received an address reported as valid that it considers invalid;
- multiple mappings were returned when only one was expected;
- incorrect service number(s) returned;
- expired data returned;
- an incorrect <uri> element was returned.

A DR against a LoST server MAY result in the LoST server reporting a discrepancy against the GIS data.

When a **LoSTDiscrepancyReport** is submitted, the "problemService" parameter is set to "LoST" and the object contains the following elements:

Name	Condition	Description
query	MANDATORY	One of the following tokens: • findService • getServiceBoundary • listServices • listServicesByLocation
request	MANDATORY	The request sent by the client (e.g., the findService request)

© Copyright 2011-2022 National Emergency Number Association, Inc.

Name	Condition	Description
response	MANDATORY	The response received by the client (e.g., the findServiceResponse)
problem	MANDATORY	One of the following tokens: • BelievedValid • BelievedInvalid • NoSuchLocation • RouteIncorrect • MultipleMappings • ServiceBoundaryIncorrect • ServiceNumberIncorrect • DataExpired • IncorrectURI • LocationErrorInError • OtherLoST

The Resolution parameter in a LoST DiscrepancyResolution report request) contains one of the following tokens:

- DiscrepancyCorrected
- DiscrepancyNotFound
- EntryAdded

3.7.6 BCF Discrepancy Report

An entity routing traffic through (to or from) a BCF (see Section 4.1) MAY report a discrepancy. The expected reports are:

- Traffic was incorrectly blocked before a dialog has been established (e.g., an INVITE, MESSAGE, or OPTIONS request, or response blocked);
- traffic was incorrectly blocked during a dialog;
- SIP signaling was inappropriately modified or dropped;
- SDP was incorrectly regenerated during B2BUA/media anchoring;
- Media was relayed with loss;
- traffic was permitted that should have been blocked because it was generated by a designated bad actor;
- traffic was permitted that should have been blocked for some other reason;
- QoS inconsistency;
- Invalid or improper Call Detail Recording;
- TTY to RTT transcoding errors;
- Firewall (non SIP) errors.

© Copyright 2011-2022 National Emergency Number Association, Inc.

When a **BCFDiscrepancyReport** is submitted, the "problemService" parameter is set to "BCF" and the object contains the following elements:

Name	Condition	Description
request	Conditional: REQUIRED when the discrepancy concerns a dialog	If the discrepancy concerns a dialog, the initial INVITE that initiated the dialog
problem	MANDATORY	One of the following tokens: • InitialTrafficBlocked • MidTrafficBlocked • BadSDP • BadSIP • MediaLoss • TrafficNotBlockedBadActor • TrafficNotBlocked • QoS • BadCDR • TTY • Firewall • OtherBCF
sosSource	MANDATORY	The emergency-source parameter of the dialog request (i.e., the initial INVITE)
eventTimestamp	MANDATORY	Timestamp of event being reported
packetHeader	Conditional, REQUIRED for InitialTrafficBlocked, MidTrafficBlocked, TrafficNotBlockedBadActor, TrafficNotBlocked, or Firewall, OPTIONAL otherwise	For InitialTrafficBlocked, MidTrafficBlocked, TrafficNotBlockedBadActor, TrafficNotBlocked, or Firewall, contains the packet's header, encoded using base64

The Resolution parameter in a BCF DiscrepancyResolution report contains one of the following tokens:

- DiscrepancyCorrected
- PerPolicy (behavior was per policy, hence not a discrepancy)
- NoDiscrepancy
- OtherResponse

© Copyright 2011-2022 National Emergency Number Association, Inc.

3.7.7 Logging Service Discrepancy Report

A Session Recording Client (SRC) or any entity generating logging events to, or retrieving logging records from, a Logging Service (see Section 4.12) MAY report a discrepancy. The expected reports are:

- An SRC encountered an error inviting the SRS;
- LogEvent returned an error when it shouldn't have;
- RetrieveLogEvent returned an error when it shouldn't have.

When a **LoggingDiscrepancyReport** is submitted, the "problemService" parameter is set to "Logging Service" and the object contains the following elements:

Name	Condition	Description
request	MANDATORY	The SIP INVITE or other request, or the LogEvent request, or the RetrieveLogEvent request
problem	MANDATORY	One of the following tokens: • InviteSRSerror • LogEventError • RetrieveLogEventError • OtherLogging
result	MANDATORY	The status code returned from the SIP request, the LogEvent request, or the RetrieveLogEvent request
callId	Conditional: REQUIRED if problem relates to a specific call	The Call Identifier
incidentId	Conditional: REQUIRED if problem relates to a specific incident	The Incident Tracking Identifier

The resolution parameter in a DiscrepancyResolution report request) contains one of the following tokens:

- DiscrepancyCorrected
- NoDiscrepancy
- OtherResponse

© Copyright 2011-2022 National Emergency Number Association, Inc.

3.7.8 PSAP Call Taker Discrepancy Report

A PSAP, downstream agency, or other entity MAY report a discrepancy against a PSAP Call Taker when a call is received that should not have been transferred to the reporting entity.

When a **CallTakerDiscrepancyReport** is submitted, the "problemService" parameter is set to "CallTaker", the "Comment" parameter contains further explanation as to why the call transfer was in error, and the "object contains the following elements:

Name	Condition	Description
CallId	MANDATORY	The Call ID assigned to the call
IncidentId	MANDATORY	The Incident ID associated with the call
pidfLO	MANDATORY	The PIDF-LO received with or via the call
callHeader	MANDATORY	The header field of the INVITE or MESSAGE

The resolution parameter in a DiscrepancyResolution report contains one of the following tokens:

- CallTakerAdvised (the call taker who transferred the call has been advised that the transfer was in error)
- TransferCorrect (the transfer was correct)
- NoDiscrepancy
- OtherResponse

3.7.9 SIP Discrepancy Report

Any entity encountering an error communicating with another entity via SIP (such as a PSAP) MAY report a discrepancy. The source of the discrepancy might be an element within or in front of the problem entity (e.g., a BCF or ESRP) that might not be visible to the entity reporting the discrepancy; in such cases the entity accepts the DR and reports its own against the responsible entity.

The expected reports are:

- An initial INVITE request failed;
- A MESSAGE request failed;
- An OPTIONS request failed;
- A SIP request sent within a dialog (e.g., a re-INVITE or INFO) failed;
- Required media stream (audio, text, video) failed to be accepted;
- Media problems during a dialog;
- Signaling failure.

© Copyright 2011-2022 National Emergency Number Association, Inc.

When a **SIPDiscrepancyReport** is submitted, the "problemService" parameter is set to "SIP" and the object contains the following elements:

Name	Condition	Description
problem	MANDATORY	One of the tokens: • InitialINVITE • MESSAGE • OPTIONS • MidDialog • RequiredMedia • MediaProblem • EngorgedQ (a queue is fuller than it should be) • Signaling • OtherSIP
callId	Conditional: REQUIRED if problem is related to a specific call	The Call Identifier
incidentId	Conditional: REQUIRED if an IncidentID is available	The Incident Tracking Identifier
testCallGenerator	Conditional: REQUIRED if DR is related to a test call	The block of parameters specified in Section 4.6.17
request	Conditional: REQUIRED if the problem occurred on a SIP request or response	The SIP request
result	Conditional: REQUIRED if the problem occurred on a SIP request or response	The status code returned from the SIP request
queueName	Conditional: REQUIRED if the call was sent to a queue	The queue in question

The Resolution parameter in a DiscrepancyResolution report contains one of the following tokens:

- DiscrepancyCorrected
- NoDiscrepancy
- OtherResponse

© Copyright 2011-2022 National Emergency Number Association, Inc.

3.7.10 Permissions/Security/Authentication Discrepancy Report

Any entity encountering a security issue or a permissions or authentication error that is believed to be incorrect, MAY report a discrepancy using the DR interface of the entity or element believed to be responsible for the discrepancy.

The expected reports are:

- Unable to authenticate;
- Unable to SUBSCRIBE to an event package;
- Permitted to SUBSCRIBE to an event package when it should have been denied;
- Unable to read a resource;
- Unable to write/modify a resource;
- Unable to delete a resource;
- Able to read a resource when it should have been denied;
- Able to write/modify a resource when it should have been denied;
- Able to delete a resource when it should have been denied;
- Unable to establish secure communication (e.g., TLS certificate invalid or TLS failure)
- Unable to verify digital signature of a resource (e.g., a routing policy signature verification failed or the certificate chain is invalid or contains an untrusted authority).

When a **PermissionsDiscrepancyReport** is submitted, the "problemService" parameter is set to "Permissions" and the object contains the following elements:

Name	Condition	Description
problem	MANDATORY	One of the tokens: • UnableAuthenticate • UnableSubscribe • AbleSubscribe • UnableRead • UnableWrite • UnableDelete • AbleRead • AbleWrite • AbleDelete • OtherPermissions (details MUST be provided in Comment field)
resource	MANDATORY	The resource being SUBSCRIBEd, read, written/modified, or deleted, or at which

© Copyright 2011-2022 National Emergency Number Association, Inc.

Name	Condition	Description
		authentication failed (URL if available)
identity	MANDATORY	AgentID (Agent Identifier, Agent Id or AgencyID (Agency Identifier, AgencyId of entity that attempted the action
result	MANDATORY	The result returned from the requested operation
detail	OPTIONAL	Provides more detail (e.g., specifics of the security failure)

The resolution parameter in a DiscrepancyResolution report contains one of the following tokens:

- DiscrepancyCorrected
- PerPolicy
- BadCertificateChain
- NoDiscrepancy
- OtherResponse

3.7.11 GIS Discrepancy Report

A LoST server or other entity MAY report a discrepancy report against GIS data. Expected reports include a gap or overlap discovered when data is coalesced, incorrect information (such as the LoST server to query for information about an area), or bad GIS data (such as bad geometry, duplicate attributes, omitted mandatory information, incorrect data type, an address range issue on centerline, a general provisioning failure, or a malformed URI).

When a **GISDiscrepancyReport** is submitted, the "problemService" parameter is set to "GIS" and the object contains the following elements:

Name	Condition	Description
problem	MANDATORY	One of the following tokens: • Gap[20] • Overlap[20]

[20] There is a gap/overlap event package used by the ECRF/LVF to notify its provisioning source of gaps or overlaps, because immediate response is required. The DR may be used to report the problems to others, such as from an SI entity to the GIS data source.

© Copyright 2011-2022 National Emergency Number Association, Inc.

Name	Condition	Description
		• IncorrectLoST • BadGeometry • DuplicateAttribute • OmittedField • IncorrectDataType • AddressRange • GeneralProvisioning • MalformedURI • DisplayData (call taker noted inaccuracies in the GIS data used in the PSAP's map display) • OtherGIS
layerIds	Conditional: REQUIRED if the error is specific to a layer or set of layers	The IDs of the layers as a white-space separated list
location	Conditional: REQUIRED if the error is specific to a location or set of locations	One or more locations where the gap or overlap can be found or for which an incorrect LoST referral is made
lostUri	Conditional: REQUIRED if a URI was provisioned	The URI provisioned
detail	Conditional: REQUIRED if the problem is an item that is duplicated, omitted, or contains an incorrect data type; or if the problem concerns bad geometry, an incorrect address range, or a malformed URI.	A string containing the name of the item that is duplicated, omitted, or contains an incorrect data type; or the geometry or address range is bad; or the URI is malformed

© Copyright 2011-2022 National Emergency Number Association, Inc.

The Resolution parameter in a DiscrepancyResolution report contains one of the following tokens:

- DataCorrected
- NoDiscrepancy
- OtherResponse

3.7.12 LIS Discrepancy Report

Any client of a LIS MAY report a discrepancy. Examples include a service provider that finds a discrepancy in the LIS' provisioning records, a client (such as an originating device) unable to obtain its own location value or reference, a client (such as an ESRP or PSAP) unable to resolve a location reference or receiving a badly formed PIDF-LO, or a PSAP call taker receiving an incorrect civic address (as verified by the call taker with the caller).

When a **LISDiscrepancyReport** is submitted, the "ProblemService" parameter is set to "LIS" and the object contains the following elements:

Name	Condition	Description
problem	MANDATORY	One of the following tokens: • IncorrectRecords • OwnLocationUnavailable • LocationReferenceNotResolved • BadPIDFLO • IncorrectLocation (incorrect civic location supplied with wireline (fixed) call) • OtherLIS
ownLocationRequest	Conditional: REQUIRED when problem is OwnLocationUnavailable	The request sent by a device for its own location
locationUrn	Conditional: REQUIRED when a location was returned by reference	The location reference
pidfLo	Conditional: REQUIRED for BadPIDFLO, SHOULD be supplied when a location was returned by value	The (possibly badly formed) PIDF-LO

© Copyright 2011-2022 National Emergency Number Association, Inc.

The Resolution parameter in a DiscrepancyResolution report contains one of the following tokens:

- RecordsCorrected
- PermissionsCorrected
- DeviceConfigError
- PerPolicy
- NoDiscrepancy
- OtherResponse

3.7.13 Policy Discrepancy Report

Any entity (such as an ESRP) using a policy (such as a routing policy) MAY report a discrepancy against the owner of the policy (e.g., a PSAP or an ESRP). For example, an ESRP or ECRF MAY report a routing policy that results in an invalid route URN, or routes to an unknown PSAP, or where the route conflicts with other policies. A PSAP receiving an incorrectly routed call MAY report that a policy is causing calls to be routed to it in error. A Policy Store MAY report a policy that is malformed or creates a loop or that fails signature verification. Any Policy Enforcement Point MAY report a policy that is malformed or conflicting or that fails signature verification.

When a **PolicyDiscrepancyReport** is submitted, the "problemService" parameter is set to "Policy" and the object contains the following elements:

Name	Condition	Description
problem	MANDATORY	One of the following tokens: • InvalidURN • UnknownPSAP • ConflictingRoute • OtherConflict • IncorrectURN • Malformed • Loop • VerificationFailure • OtherPolicy (details REQUIRED in the Comment field)
policyId	MANDATORY	The policy ID
location	Conditional: REQUIRED if DR is against a PRR policy	The location

© Copyright 2011-2022 National Emergency Number Association, Inc.

Name	Condition	Description
callId	Conditional: REQUIRED if DR is specific to a call	Call Tracking Identifier
routeUrn	Conditional: REQUIRED if DR is against a PRR policy	The route URN

The Resolution parameter in a DiscrepancyResolution report contains one of the following tokens:

- PolicyCorrected
- NoError
- NoDiscrepancy
- OtherResponse

3.7.14 Originating Service Provider Discrepancy Report

An entity MAY report a discrepancy against an Originating Service Provider when a location provided by the Originating Service Provider fails validation. An ECRF or ESRP or PRF or PSAP MAY report a discrepancy when a default location is used for routing because location is missing or not usable. An LNG or other entity MAY report a call received without ANI. An LNG or ESRP or other entity MAY report that a badly formed PIDF-LO was received or a location query timed out without receiving a PIDF-LO. An LSRG or other entity MAY report that a call was dropped or terminated without appropriate signaling. A PSAP MAY report a discrepancy when a civic location received with a fixed (wireline) call is incorrect. A BCF, ESRP, PSAP, or other entity MAY report an incorrectly formed call (e.g., a SIP INVITE that is badly formed, lacks certain header fields or body parts, etc.). A BCF, ESRP, PSAP, or other entity, MAY report that an unusually large call volume (which might suggest a DoS or other attack) or an unusually low call volume is being generated by the Originating Service Provider. An Originating Service Provider MAY report a discrepancy against itself to raise an issue to be addressed. An entity MAY report a discrepancy when an Additional Data reference included in the call is invalid. An entity MAY report a discrepancy when an Additional Data value is invalid. The Secure Telephone Identity-Verification Service (STI-VS) FE [ref Section 4.21] MAY report a Secure Telephone Identity verification failure to an Originating Network.

Note: A Discrepancy Report by an OSP toward the OCIF reporting an identity verification failure for a call from the OCIF will be addressed in a future edition of this document.
When an **OriginatingServiceDiscrepancyReport** is submitted, the "problemService" parameter is set to "OriginatingService" and the object contains the following elements:

© Copyright 2011-2022 National Emergency Number Association, Inc.

Name	Condition	Description
problem	MANDATORY	One of the following tokens: • LocationNotLVFValid • LocationMissing • NoANI • BadPIDFLO • QueryTimeOut • CallDropped • IncorrectLocation • BadSIP (problem details REQUIRED in Comment field) • CallDrought • CallFlood (service provider is sending too many calls, there may be a DoS attack, or other problem to investigate) • InvalidADR • BadAdditionalData • OtherOSP • STIerror
status	Conditional: REQUIRED when using InvalidADR or STIerror	For InvalidADR, the status code returned with the rejection of the ADR dereference attempt. For STIerror, the status code returned in the Reason header field when the STI Verification Service (STI-VS) encounters a validation failure (see Section 4.21.1)
location	Conditional: REQUIRED when DR relates to location associated with the call	The location value or reference provided by the Originating Service Provider. If there is no location, leave empty.
locationId	Conditional: REQUIRED when DR relates to location associated with the call	The client or endpoint identifier provided with the location

© Copyright 2011-2022 National Emergency Number Association, Inc.

Name	Condition	Description
locationCorrect	Conditional: REQUIRED when DR relates to location associated with the call	One of the following tokens: • True (location received with the call is correct as verified by call taker with caller) • False (location received with the call is incorrect as verified by call taker with caller) • Unknown
callHeader	Conditional: REQUIRED when DR relates to a SIP header field	The header field of the INVITE or MESSAGE
callVolume	Conditional: REQUIRED when using CallDrought or CallFlood	The number of calls received within a measured period of time
callVolumeTimePeriod	Conditional: REQUIRED when using CallDrought or CallFlood	The period of time in seconds during which CallVolume calls were received

The Resolution parameter in a DiscrepancyResolution report contains one of the following tokens:

- ProblemCorrected
- InvalidRecord
- NoDiscrepancy
- OtherResponse

3.7.15 Call Transfer Failure Discrepancy Report

A PSAP, LSRG, or other entity MAY report a discrepancy against a transfer entity when a transfer fails. The notification SHOULD be made to both the entity originating the transfer and the entity receiving the transfer.

When a **CallTransferDiscrepancyReport** is submitted, the "problemService" parameter is set to "CallTransfer" and the object contains the following elements:

Name	Condition	Description
callId	MANDATORY	The Call ID assigned to the call
incidentId	MANDATORY	The Incident ID associated with the call

© Copyright 2011-2022 National Emergency Number Association, Inc.

Name	Condition	Description
origin	MANDATORY	The AgencyID of the originator of the transfer
status	MANDATORY	The status code received during the transfer attempt
destination	MANDATORY	The AgencyID of the recipient of the transfer

The Resolution parameter in a DiscrepancyResolution report contains one of the following tokens:

- ProblemCorrected
- NoDiscrepancy
- OtherResponse

3.7.16 MSAG Conversion Service (MCS) Discrepancy Report

An LSRG or other entity MAY report a discrepancy against the MSAG Conversion Service (MCS) when a conversion fails, but the querier believes it should have succeeded. A DR MAY also be filed when the conversion succeeded but the returned location from the MCS is not MSAG-valid or LVF-valid. Both these errors can occur in either direction (PIDF-LO to MSAG or MSAG to PIDF-LO).

When an **MCSDiscrepancyReport** is submitted, the "problemService" parameter is set to "MCS" and the object contains the following elements:

Name	Condition	Description
ServiceCall	MANDATORY	One of the tokens: • PIDFLOtoMSAG • MSAGtoPIDFLO
pidfLo	MANDATORY	The PIDF-LO supplied to PIDFLOtoMSAG, or received from MSAGtoPIDFLO
msag	MANDATORY	The MSAG supplied to MSAGtoPIDFLO, or received from PIDFLOtoMSAG
Referral	Conditional: REQUIRED when a Referral to another MCS was returned	Referral value received from MCS
statusCode	MANDATORY	The status code received from the conversion attempt

© Copyright 2011-2022 National Emergency Number Association, Inc.

The Resolution parameter in a DiscrepancyResolution report contains one of the following tokens:

- ProblemCorrected
- NoDiscrepancy
- OtherResponse

3.7.17 ESRP Discrepancy Report

A PSAP or other entity MAY report a discrepancy against an ESRP when a call is received that should not have been routed to the PSAP, or the ESRP has one or more queues whose fullness is a problem, or if the PSAP seems to be receiving fewer calls than would normally be expected. A routing problem may be the result of incorrect data in the ECRF (GIS data). Calls are sent to PSAPs by ESRPs, so a PSAP should report a problem to the ESRP. The ESRP, in turn, reports any suspected GIS problems to the ECRF.

When an **ESRPDiscrepancyReport** is submitted, the "problemService" parameter is set to "ESRP" and the object contains the following elements:

Name	Condition	Description
problem	MANDATORY	One of the following tokens: • CallReceived • EngorgedQ • CallDrought
callId	Conditional: REQUIRED when DR relates to a specific call	The Call ID assigned to the call
incidentId	Conditional: REQUIRED when DR relates to a specific Incident	The Incident ID associated with the call
pidfLo	Conditional: REQUIRED when the DR relates to a specific call	The PIDF-LO received with or via the call
queueName	Conditional: REQUIRED when the DR is due to one or more queues whose fullness is a problem; OPTIONAL when the DR is due to the PSAP receiving fewer calls than would normally be expected	The queue in question

© Copyright 2011-2022 National Emergency Number Association, Inc.

The Resolution parameter in a DiscrepancyResolution report contains one of the following tokens:

- ProblemCorrected
- GIS (GIS data incorrect; GIS DR filed)
- PerPolicy
- NoDiscrepancy
- OtherResponse

3.7.18 ADR/IS-ADR Discrepancy Report

A PSAP, ESRP, ECRF, or other entity or function MAY report a discrepancy against an ADR or IS-ADR.

When an **AdrDiscrepancyReport** is submitted, the "problemService" parameter is set to "ADR" and the object contains the following elements:

Name	Condition	Description
problem	MANDATORY	One of the following tokens: • ReferenceNotResolved • Malformed • UnknownBlock • ReceivedIncorrectData (as verified by call taker with caller) • TooManyURIs (reported when an ECRF is provisioned with more URIs for a location than can be returned) • OtherADR
block	Conditional: REQUIRED if the problem relates to a specific block	The name of the block
location	Conditional: REQUIRED when a location was used to search for Additional Data	The location used to search for the Additional Data
identity	Conditional: REQUIRED for IS-ADR (as opposed to ADR)	The identity used to search for the additional data

© Copyright 2011-2022 National Emergency Number Association, Inc.

Name	Condition	Description
url	Conditional: REQUIRED for ADR (as opposed to IS-ADR)	The additional data URI
result	Conditional: REQUIRED if a result was received from the ADR/IS-ADR	The result received from the ADR/IS-ADR

The Resolution parameter in a DiscrepancyResolution report contains one of the following tokens:

- ProblemCorrected
- NoDiscrepancy
- OtherResponse

3.7.19 Network Discrepancy Report

Any entity MAY report a general networking discrepancy. For example, any entity MAY report a discrepancy with general network facilities (such as DNS or DHCP failure, high latency, packet loss, or routing failure) within an ESInet or PSAP. ESInet and PSAP operators MUST support receiving such DRs; other operators MAY support receiving them.

When a **NetworkDiscrepancyReport** is submitted, the "problemService" parameter is set to "Network" and the object contains the following elements:

Name	Condition	Description
problem	MANDATORY	One of the following tokens: • TimeoutDNS • IncorrectDNS (incorrect results) • TimeoutDHCP • IncorrectDHCP (incorrect results) • PacketLoss • PacketLatency • Routing • OtherNetwork (details MUST be provided in Comment field)
iPAddressLocal	Conditional: REQUIRED unless DHCP related and IP address not available	The IP address of the machine experiencing the error

© Copyright 2011-2022 National Emergency Number Association, Inc.

Name	Condition	Description
ipAddressRemote	Conditional: REQUIRED unless problem is DNS or DHCP related	The IP address to/from which the problem is occurring
url	Conditional: REQUIRED if known	The URL of the resource (e.g., the DNS or DHCP server)
timestamp	MANDATORY	The time at which the problem occurred

The Resolution parameter in a DiscrepancyResolution report containsnone of the following tokens:

- ProblemCorrected
- NoDescrepancy
- OtherResponse

3.7.20 Interactive Media Response (IMR) Discrepancy Report

Any entity aware of a discrepancy at an Interactive Media Response (IMR) MAY report a discrepancy at it. For example, a PSAP or ESRP MAY report a discrepancy if the IMR has one or more queues whose fullness is a problem, a call taker MAY report a discrepancy if the caller reports that an incorrect or confusing message was played, a call was transferred incorrectly, the caller experienced excessive silence, or another script error occurred.

When an **IMRDiscrepancyReport** is submitted, the "problemService" parameter is set to "IMR" and the object contains the following elements:

Name	Condition	Description
problem	MANDATORY	One of the following tokens: • EngorgedQ • ResponseIncorrect • ResponseConfusing • CallTransferIncorrect • ExcessiveSilence • UnknownScript • InputFailed (e.g., DTMF failure) • ScriptLogicFailure • OtherIMR (details MUST be provided in Comment field)
callId	MANDATORY	The Call ID assigned to the call

© Copyright 2011-2022 National Emergency Number Association, Inc.

Name	Condition	Description
incidentId	Conditional: REQUIRED if used for an emergency call	The Incident ID associated with the call
callHeader	MANDATORY	The header field of the INVITE or MESSAGE

The Resolution parameter in a DiscrepancyResolution report contains one of the following tokens:

- ProblemCorrected
- NoDescrepancy
- OtherResponse

3.7.21 Test Call Generator Discrepancy Report

When a Test Call Generator encounters errors initiating or processing a test call, it reports the discrepancy to the PSAP that should have received the test call.

Note that a Test Call Generator might create other DRs in addition to or instead of this DR, and a PSAP that receives a test call might create DRs in response to the test call. For example, a Test Call Generator might file a SIP or IMR DR against a receiving PSAP whether or not it is the expected PSAP, as problems in its handling of the test call could warrant generating a DR against it regardless. Similarly, a Test Call Generator or a PSAP that receives a test call might create a Policy or ESRP DR if the test call was routed unexpectedly.

The expected cases for this Discrepancy Report are:

- an initial INVITE request failed;
- a MESSAGE request failed;
- an OPTIONS request failed;
- a SIP request sent within a dialog (e.g., a re-INVITE or INFO) failed;
- loopback media stream (audio, text, video) failed to be accepted;
- loopback media problems during the test dialog;
- signaling failure.

When a **TestCallDiscrepancyReport** is submitted, the "problemService" parameter is set to "TestCall" and the object contains the following elements:

Name	Condition	Description
problem	MANDATORY	One of the tokens: • TestINVITE

© Copyright 2011-2022 National Emergency Number Association, Inc.

Name	Condition	Description
		• TestMESSAGE • TestOPTIONS • TestMidDialog • TestMedia • TestLoopbackMedia • TestSignaling • TestCallOther
callId	MANDATORY	The Call Identifier
request	MANDATORY	The SIP request
result	MANDATORY	The status code returned from the SIP request
nbrOfCalls	MANDATORY	Number of test calls placed since the last time SendCallRequests was received from this PSAP (as an integer)
successCount	MANDATORY	Number of calls counted in NbrOfCalls that were completed successfully (as an integer)
failCount	MANDATORY	Number of calls counted in NbrOfCalls that were attempted, but failed to complete (as an integer)

The Resolution parameter in a DiscrepancyResolution report contains one of the following tokens:

- ProblemCorrected
- NoDescrepancy
- OtherResponse

3.7.22 Log Signature/Certificate Discrepancy Report

When an entity (e.g., a Logging Service or another entity) that verifies LogEvent signatures is unable to obtain a certificate, encounters an invalid certificate or thumbprint, or the signature verification fails, it reports the discrepancy to the entity that generated the LogEvent.

The expected cases for this Discrepancy Report are:

- the certificate cannot be obtained (no "x5c" nor "x5u" field provided);

© Copyright 2011-2022 National Emergency Number Association, Inc.

- the "x5u" field cannot be resolved or does not resolve to a valid certificate;
- the "x5u" field is present but the "x5t#256" field is missing, or the thumbprint specified does not match the certificate obtained from the "x5u" field;
- the signature of a LogEvent does not verify.

When a **LogSignDiscrepancyReport** is submitted, the "problemService" parameter is set to "LogSign" and the object contains the following elements:

Name	Condition	Description
problem	MANDATORY	One of the tokens: • BadAlgorithm ("alg" header was not set to "ES256") • NoCert (neither "x5u" nor "x5c" fields present) • BadURL (unable to resolve the "x5u") • BadThumb (an "x5u" field was present, but the "x5t#S256" field is either missing or doesn't match the certificate obtained by resolving the "x5u" field) • BadCertX5c (invalid certificate in the "x5c" field) • BadCertX5u (invalid certificate obtained via the "x5u" field) • BadSignature (unable to verify signature) • OtherLogSignature
logEventId	MANDATORY	The logEventId of the LogEvent.
result	Conditional: REQUIRED if Problem is BadURL	The response received when resolving the "x5u" field.
thumbCalc	Conditional: REQUIRED if Problem is BadThumb	The thumbprint calculated from the certificate

The Resolution parameter in a DiscrepancyResolution report contains one of the following tokens:

- ProblemCorrected

© Copyright 2011-2022 National Emergency Number Association, Inc.

- NoDescrepancy
- OtherResponse

4 Functions

4.1 Border Control Function (BCF)

A BCF MUST be deployed between external networks and the ESInet/NGCS. A BCF SHOULD be deployed between the ESInet/NGCS and agency networks. The latter may be provided by the NGCS operator or may be provided by the PSAP, or both.

4.1.1 Functional Description

The BCF comprises several distinct elements pertaining to network edge control and SIP message handling. These include:

- Border Firewall
- Session Border Control
- Call Suspicion/Bad Actor functions

The BCF MUST support the following security related techniques:

- Prevention
- Detection
- Reaction

Additionally, the entirety of the functional element MAY include aspects of the following:

- SIP B2BUA
- Media anchoring
- Stateful Firewall

Border Firewall — this functional component of the BCF inspects ingress and egress traffic running through it. It is a dedicated appliance or software running on a computer. There are a variety of different roles a firewall can take; however, the typical roles are application layer and network layer firewalls:

1) Application layer – these scan and eliminate known malware attacks from extranet and intranet sources at OSI layer 7 before they ever reach a user's workstation or a production server or another end point located inside the ESInet. These act as the primary layer of defense for most malware attacks that are protocol specific.
2) Network layer — these manage access on the network perimeter and between network segments. Typically, they do not provide active scanning at the application layer and provide access control through the use of access control lists and port-

© Copyright 2011-2022 National Emergency Number Association, Inc.

based permission/denial management (UDP, TCP etc.). They also mitigate attacks on lower layer protocol layers (e.g., TCP SYN Flooding).

Firewalls deployed on the ESInet SHALL meet the following specifications:

1) Provide both application and network layer protection and scanning;
2) Denial of Service (DoS) detection and protection;
    a. Detection of unusual incoming IP packets that may then be blocked to protect the intended receiving user or network;
    b. To prevent distributed denial of service (DDoS) attacks, destination specific monitoring, regardless of the source address, may be necessary.
3) Provide a mechanism such that malware definitions and patterns can be easily and quickly updated by a national 9-1-1 Computer Emergency Response Team (CERT) or other managing authority;
4) Capability to receive and update 9-1-1 Malicious Content (NMC) filtering automatically for use by federated firewalls in protecting multiple disparate ESInets.

Please refer to NENA 04-503 [71] for more information on firewall requirements.

Session Border Control — The session border controller functional element of the BCF plays a role by controlling borders to resolve problems such as Network Address Translation (NAT) or firewall traversal. Session Border Controllers (SBCs) are already being extensively used in existing service provider networks.

Commercial Off The Shelf SBCs and Firewalls may be extended to have NGCS-specific capability, or a separate functional component may provide that functionality.

The following primary functions are related to the SBC (or the NGCS-specific functional component within a BCF:

- Identification of emergency call/session and priority handling for the IP flows of emergency call/session traffic. Use of the SBC or any other ESInet element for non-emergency calls that enter an ESInet is not described herein except for calls to an administrative number in the PSAP. Such non-emergency calls are beyond the scope of this document.
- Conformance checking and mapping (if applicable) of priority marking based on policy for emergency calls/sessions.
- Facilitate forwarding of an emergency call/session to an ESRP (and only an ESRP).
- Adding Call and Incident Tracking identifiers to the signaling.
- Adding the Resource-Priority header field if not already included.
- Protection against DDoS attacks: The SBC component of the BCF shall protect against SIP specific and general DDoS attacks.
- Implementing the "Bad Actor" mechanism as described in Section 4.1.2.

© Copyright 2011-2022 National Emergency Number Association, Inc.

- SIP Protocol Normalization: The SBC component of the BCF SHALL support SIP/SDP protocol normalization and/or repair, including adjustments of encodings to a core network profile. This may be done in order to facilitate backward compatibility with older devices that may support a deprecated version of SIP/SDP. The "lr" parameter should be added to the routing URIs if not already present.
- NAT and Network Address and Port Translation (NAPT) Traversal: The SBC component of the BCF SHALL perform NAT traversal for authorized calls/sessions using the SIP protocol. The SBC component MUST be able to recognize that a NAT or NAPT has been performed on Layer 3 but not above and correct the signaling messages for SIP.
- IPv4/IPv6 Interworking: The SBC component of the BCF SHALL enable interworking between networks utilizing IPv4 and networks using IPv6 through the use of dual stacks, selectable for each SBC interface. All valid IPv4 addresses and parameters SHALL be translated to/from the equivalent IPv6 values.
- Signaling Transport Protocol Support: The SBC component of the BCF SHALL support SIP over the following protocols: TCP, UDP, TLS-over-TCP, and SCTP. Protocols supported MUST be selectable for each SBC interface to external systems. These transport layer protocols are generated and terminated at each interface to external systems (i.e., there is no "pass-thru" of transport layer information). The signaling for all calls entering the ESInet should be protected over TLS using AES-256 or better. The SBC component of the BCF MUST use TLS with AES-256 or better towards the ESInet.
- VPN Bridging or Mediation: The SBC component of the BCF SHALL support terminating the IP signaling received from a foreign carrier onto the ESInet address space. The SBC component of the BCF SHALL support B2BUA functions to enable VPN bridging if needed.
- QoS/Priority Packet Markings: The SBC component of the BCF SHALL be capable of populating the layer 2 and layer 3 headers/fields, based on call/session type (e.g., 9-1-1 calls) in order to facilitate priority routing of the packets.
- Call Detail Records: The SBC component of the BCF SHALL be capable of producing CDRs based on call/session control information (e.g., SIP/SDP). These CDRs can be used to manage the network and for Service Level Agreement (SLA) auditing.
- Transcoding: The SBC component of the BCF MAY support transcoding. For example, the SBC component MAY transcode Baudot tones to RFC 4103 [85] real-time text. See Section 3.1.9.3.
- Media Protection: The media of all calls entering the ESInet should be protected against eavesdropping, alteration, and replay using SRTP with AES-256 or better. All media connections exiting the SBC towards the ESInet MUST be protected against eavesdropping, alteration, and replay using AES-256 or better. An SBC component

© Copyright 2011-2022 National Emergency Number Association, Inc.

of the BCF which always anchors media achieves this by accepting any media, with SRTP or not, and MUST protect the media towards the ESInet. An SBC that does not routinely anchor media MUST anchor media for calls entering without sufficient protection (AES-256 or better) and MUST protect the media towards the ESInet.

Additionally, the SBC component of the BCF SHALL perform the following functions:

- Opening and closing of a pinhole (firewall)
  - Triggered by signaling packets, a target IP flow is identified by "5-tuples" (i.e., source/destination IP addresses, source/destination port number, and protocol identifier) and the corresponding pinhole is opened to pass through the IP flow.
- Resource and admission control
  - For links directly connected to the element, and OPTIONALLY networks behind the element, resource availability is managed and admission control is performed for the target call/session.
- IP payload processing
  - Transcoding (e.g., between G.711 and G.729) and DTMF interworking.
- Performance measurement
  - Quality monitoring for the target IP flow in terms of determined performance parameters, such as delay, jitter, and packet loss. Performance results may need to be collected for aggregated IP flows.
- B2BUA for UAs that do not support Replaces
  - The SBC component MAY include a B2BUA function for 9-1-1 calls in which the caller does not indicate support for the Replaces operation. See Section 4.7.1.2.

Typically, the firewall passes traffic for inbound SIP protocol to the Session Border Controller, which acts as an Application Layer Gateway for SIP. Primary non-SIP protection is accomplished by the Firewall functions of the BCF. Primary SIP protection is accomplished by the SBC component of the BCF.

BCFs between the NGCS and a PSAP only need some of the above functionality.

4.1.2 Interface Description

The BCF supports SIP interfaces upstream and downstream per Section 3.1. The BCF, as the first active SIP element in the path of an emergency call, MUST add to the call the NENA Call Identifier, NENA Incident Tracking Identifier and a SIP Resource-Priority header field with a value from the "esnet" namespace (if not already present). These identifiers MUST be added to the initial message of a dialog forming transaction (INVITE) or the MESSAGE method associated with a non-interactive call. The identifiers SHOULD be added to all other SIP messages presented to the NGCS. The BCF SHALL police SIP Resource-Priority to appropriate values in the "esnet" namespace (See Section 3.1.7).

© Copyright 2011-2022 National Emergency Number Association, Inc.

The BCF SHALL support an automated interface that allows a downstream element to mark a particular source of a call as a "bad actor" (usually due to receipt of a call that appears to be part of a deliberate attack on the system) and send a message to the BCF notifying it of this marking. To facilitate this notification, the BCF SHALL insert a Call-Info header field with a purpose parameter of "emergency-source" in the outgoing INVITE message associated with every call. Because the SBC component of the BCF MAY rewrite addresses, calls MUST be marked by the SBC component in a way that allows the recipient to identify the BCF that processed the call. The source-ID is formatted as follows: <unique source-id>@<domain name of BCF> (e.g., "a7123gc42@sbc22.example.net"). It is common to have more than one SBC for a particular call source. The notification MUST be propagated to all such SBCs. The mechanism for doing so is not specified.

Note: this construction does not specify a scheme and the lack of a scheme is not conformant to RFC 3261. This will be fixed in a future version of this document.

Note: This construction does not conform to RFC 3261 (which requires a proper URL with a scheme). This will be addressed in a future version of this document.

When the downstream element identifies a source as a "bad actor", it signals the BCF as to which source is misbehaving by sending it a BadActorRequest that contains the sourceId from the Call-Info header field with a 'purpose' parameter of "emergency-source" of the incoming INVITE message or MESSAGE request. The BCF responds by returning a BadActorResponse message that indicates whether or not an error was detected in the BadActorRequest message.

Upon receiving the BadActorRequest, the SBC component of the BCF SHOULD, subject to local regulation, filter out subsequent calls from that source until the attack subsides. Provisioning determines whether the BCF deploys BadActor filtering. As an alternative to blocking calls, the Call Suspicion score (see Section 4.1.2.1 may be raised by a provisioned value.

Note that blocking of emergency calls is a complex issue that may involve local regulation, liability issues and other legal implications. Use of this function may be restricted by such issues. Also note that a rogue actor within an ESInet could hinder calls for one or more PSAPs inappropriately. The BCF SHOULD restrict access to the mechanism to entities with a PSAP agency type in their PCA-traceable certificates. Source-Ids MUST be unguessable. If the BCF does not recognize the source-id, it MUST ignore the request.

HTTP method: POST

Resource name .../BadActors

© Copyright 2011-2022 National Emergency Number Association, Inc.

The request body contains the Bad Actor source-id as a string

Status Codes

201	Bad Actor successfully added
401	Unauthorized
432	Already reported
433	No such sourceId
454	Unspecified Error

BCFs that anchor media MUST implement the Session Recording Client interface defined by SIPREC (RFC 7866) [116]. Provisioning MAY control whether the BCF logs media.

Disabling BadActor filtering for a specific source is based on time and is implementation dependent. Frequency of calls from the source, types of calls, and prior history may determine how long the filtering is maintained.

4.1.2.1 CallSuspicion

The BCF MAY identify calls that may be part of a deliberate attack on the system. However, under normal conditions, the BCF will allow suspicious calls in, preferring to have a suspicious call show up rather than blocking a potentially legitimate call. The behavior of downstream elements (ESRPs for example) may be affected by the determination of the BCF. For this purpose, if the BCF evaluates suspicion, it SHALL insert a Call-Info header field with a purpose parameter of "emergency-CallSuspicion", with an integer value of 0-100 indicating the call suspicion score where 0 is least suspicious (i.e. no suspicion) and 100 is most suspicious. The absence of the emergency-CallSuspicion parameter in a call means no determination was made.

Note: This text does not describe how an integer is formatted in a Call-Info URL in conformance with RFC 3261. This will be addressed in a future version of this document.

4.1.3 Roles and Responsibilities

The ESInet operator is responsible for the BCF at the edge of the ESInet. PSAP or other agency is responsible for a BCF between its network and the ESInet.

4.1.4 Operational Considerations

Creation of a Public Safety Computer Emergency Response Team (CERT) is anticipated, and all BCF operators MUST arrange to receive alerts from the CERT and respond. All BCF support organizations MUST have trained staff available 24 x 7 x 365 to immediately respond to attacks and have the capability and training to be able to adjust the BCF to mitigate such attacks.

© Copyright 2011-2022 National Emergency Number Association, Inc.

4.2 Emergency Service Routing Proxy (ESRP)

4.2.1 Functional Description

4.2.1.1 Overview

The Emergency Service Routing Proxy (ESRP) is the base routing function for emergency calls for i3. As described in NENA 08-002 [70], ESRPs are used in several positions within the ESInet:

- The "Originating ESRP" is the first routing element inside the ESInet. It receives calls from the BCF at the edge of the ESInet;
- One or more "Intermediate ESRPs" which exist at various hierarchical levels in the ESInet. For example, the Originating ESRP may be a state-level function, and an intermediate ESRP may be operated by a county agency;
- The "Terminating ESRP" is typically at the edge of the NGCS, just before the PSAP BCF.

The function of the ESRP is to route a call to the next hop (the routing URI should contain the "lr" parameter to avoid Request-URI rewriting). The Originating ESRP routes to the appropriate intermediate ESRPs (if they exist), intermediate ESRPs route to the next level intermediate ESRP or to the Terminating ESRP (i.e., the appropriate PSAP). The Terminating ESRP routes to a PSAP's Call Handling and/or IMR FE.

ESRPs typically receive calls from upstream routing proxies. For the originating ESRP, this is typically a carrier routing proxy. For an intermediate or terminating ESRP, this is the upstream ESRP. The destination of the call on the output of the ESRP is conceptually a queue, represented by a Queue Identifier. In most cases, the queue is maintained on a downstream ESRP, and is most often empty. However, when the network gets busy for any reason, it is possible for more than one downstream element to "pull" calls from the queue. The queue is most often First In First Out, but in some cases there can be out-of-order selections from the queue.

The primary input to an ESRP is a SIP message. The output is a SIP message with a Route header field (possibly) rewritten (this URI should contain the "lr" parameter to avoid Request-URI rewriting), a Via header field added, and in some cases, additional manipulation of the SIP messages. In order for the Policy Routing Function (PRF) to evaluate and execute its rules, the ESRP has interfaces to the ECRF (for location-based routing information), LISes and ADRs, as well as to various event notification sources to gather state information.

For typical 9-1-1 calls with a Request-URI starting with "urn:service:sos" received, the ESRP will:

© Copyright 2011-2022 National Emergency Number Association, Inc.

1) Evaluate an origination policy "rule set" (OriginationRoutePolicy) for the queue the call arrives on;
2) Query the location-based routing function (ECRF) with the location included with the call (including any steps to dereference location included by reference) to determine the "normal" next hop (smaller political or network subdivision, PSAP, or call taker group) URI[21];
3) Evaluate a policy rule set (NormalNexthopRoutePolicy) triggered by an InvokePolicyAction using other inputs available to it such as header fields in the SIP message, time of day, PSAP state, etc.

InvokePolicyAction may also be used to cause the ESRP to execute another policy (OtherRoutePolicy).

The result of the policy rule evaluation is a URI. The ESRP forwards the call to the URI (which is a queue as described above).

If the call arrives at an ESRP with no queue name or a queue name that the ESRP does not implement, the ESRP SHALL use a provisioned default queue for the call.

The ESRP also has a SIP interface to the STI-VS FE (see section 4.21.1) for the purpose of validating the telephone identity of emergency calls presented to it.

The ESRP MAY also handle calls to what used to be called "administrative lines", meaning calls directed to, for example, a 10 digit number listed for a particular PSAP, although in NG9-1-1, they may be multimedia calls, and may be to a more general SIP URI. It is recommended that such calls route through the Outbound Call Interface Function (OCIF) of the serving NGCS (potentially through an Originating ESRP) to a next-hop ESRP, and be subject to the same security and policy routing as regular 9-1-1 calls. Such calls do not have a service URN in the Request-URI line, do not have Geolocation header fields, would typically arrive on a different queue with a different origination policy, would not query an ECRF, and would use a fixed URL for "Normal-Next Hop".

It is desirable in many circumstances for calls to be policy-routed instead of being sent directly to a PSAP, that is, the INVITE or MESSAGE should be sent to the ESRP instead of directly to the PSAP. This allows for testing various conditions (e.g., ServiceState/SecurityPosture, TimeOfDay, etc.) at the PSAP prior to sending the call there. To accomplish this, it is RECOMMENDED that the URI in the ECRF for that PSAP MUST treat such calls the same way it treats all other calls arriving on queues it manages, that is, it evaluates the OriginationRoutePolicy associated with that queue. That PRR ruleset

[21] The ECRF query is invoked as part of rule evaluation. A given rule set need not invoke an ECRF query, but all ESRPs must implement the capability to query an ECRF

© Copyright 2011-2022 National Emergency Number Association, Inc.

however, should not cause an ECRF query. If calls transferred to a PSAP are to be policy-routed, then the URI in the ECRF SHALL point to a queue. Note that the responders may have URIs in the ECRF that are different from a URI found in, for example, the Agency Locator, which may follow different paths. Responders SHOULD use route policy for handling unusual circumstances that may require calls to be forwarded to alternative agencies, but they are NOT REQUIRED to do so. ESRPs which do not have a policy for the Route header field in this circumstance forward the call to the domain specified in the Route header field with no further processing.

A serving ESRP is usually the default outbound proxy for calls originated by a PSAP. When the ESRP is not configured as the default outbound proxy for the PSAP, the OCIF MAY be contacted directly, if so configured by the NGCS provider. An ESRP routes calls within the ESInet, and routes calls to destinations outside an ESInet using the OCIF. Call-backs to the original caller are an example of such outbound calls to external destinations. The ESRP routes outbound calls based on an origination policy for a provisioned ESRP queue used for calls which would route to an OCIF. While an ESRP could be an incoming proxy server for non-emergency calls, such use is beyond the scope of this standard.

Note: This section will be expanded in a subsequent version to include non-transferred calls.

4.2.1.2 Call Queuing

The destination of every routing decision is conceptually a queue of calls. The queue can be large or small, it can have one or many sources entering calls on a queue, and it can have one or many sources taking calls off the queue. All queues defined in this document are normally First In First Out, have defined maximum length and a current call-in-queue length. A unique Queue Identifier identifies a queue. A queue is normally managed by an ESRP or PSAP. A call sent to the queue URI MUST route to the entity that manages it. Calls are enqueued by forwarding them to the URI (which is usually obtained by policy rule evaluation of an upstream ESRP). Calls typically are dequeued by the ESRP, making a routing decision and sending the call to a downstream queue managed by an ESRP or PSAP. As such, all call queues are "ingress" queues, conceptually on the input side of an ESRP. In cases in which more than one dequeuer exists for a queue, one entity (normally an ESRP) manages the queue, and other ESRPs register to dequeue calls from the queue. The queue mechanism discussed here is not an "egress" queue, which would conceptually be on the output side of an ESRP. A given ESRP takes calls off its queues (or queues managed by some other entity if there are multiple dequeuers) and processes them. That ESRP will then enqueue the call on a downstream entity that manages another queue.

ESRPs may, and often will, manage multiple queues. For example, an ESRP may manage a queue that is used for normal 9-1-1 calls routed to the local ESInet, and one or more

© Copyright 2011-2022 National Emergency Number Association, Inc.

queues for calls that are diverted to it by ESRPs from other areas that are overloaded. Each queue MUST have a unique URI that routes to the ESRP. The queue length an ESRP reflects the number of calls to be routed.

In practice, some proxy servers MAY be simple RFC 3261 [10] compliant servers. In such cases, the queue is considered to have a length of 1 and its existence can be ignored.

The ESRP managing a queue may have policies controlling which entities may enqueue (Enqueuers) and dequeue (DequeueRegistration) calls to the queue. The dequeueing entity registers (DequeueRegistration) to receive calls from the queue. The ESRP would respond to a call from an entity not in its policy with a 404 error.

Each ESRP element SHALL maintain a QueueState notifier and track the number of calls in queue for the queues that it manages. Changing the ServiceState MUST change the state of all Queues implemented by the Service to an appropriate QueueState (for example if ServiceState is set to Unstaffed, underlying QueueState values become Disabled). ESRPs normally are aware of downstream queue state, but do not report such status upstream.

4.2.1.3 QueueState Event Package

QueueState is an event that indicates to an upstream entity the state of a queue. The SIP Notify mechanism described in RFC 6665 [14] is used to report QueueState. The event includes the URI of the queue, the current queue length, allowed maximum length, and a state value from the queueState registry (Section 10.17).

The registry includes the value "unreachable", which MUST NOT be returned in a NOTIFY.

QueueState is NOT REQUIRED to be implemented on simple routing proxy or when queue length is 1 and only one dequeuer is permitted. QueueState MUST reflect the state of the (ESRP or PSAP) service state. If the ESRP is down, all of its queues MUST show a state matching the reason the service is not available.

Event Package Name: emergency-QueueState

Event Package Parameters: None

SUBSCRIBE Bodies: Standard RFC 4661 [92] + extensions filter specification may be present

Subscription Duration: Default one (1) hour. One (1) minute to twenty-four (24) hours is reasonable.

NOTIFY Bodies: MIME type Application/EmergencyCallData.queuestate+json

Name	Condition	Description
queueUri	MANDATORY	SIP URI of queue

© Copyright 2011-2022 National Emergency Number Association, Inc.

Name	Condition	Description
queueLength	MANDATORY	Integer indicating current number of calls in the queue.
queueMaxLength	MANDATORY	Integer indicating maximum length of queue
state	MANDATORY	Enumeration of current queue state (e.g., Active/Inactive/Disabled)

Notifier Processing of SUBSCRIBE Requests: The Notifier (i.e., the ESRP) consults the policy (queueState) to determine if the requester is permitted to subscribe. If not, the ESRP returns 603 Decline. The ESRP determines whether the queue is one of the queues managed by the Notifier. If not, the ESRP return 488 Not Acceptable Here. If the request is acceptable, the Notifier returns 200 OK.

Notifier Generation of NOTIFY Requests: When state of the queue changes (call is placed on, removed from the queue, or management action/device failure changes the "state" enumeration), a new NOTIFY is generated, adhering to the filter requests.

Subscriber Processing of NOTIFY Requests: Specific action NOT REQUIRED.

Handling of Forked Requests: Forking between elements MUST NOT be used.

Rate of Notification: This package is designed for relatively high frequency of notifications. The subscriber can control the rate of notifications using the filter rate control (RFC 6446) [80]. The default throttle rate is one notification per second. The default force rate is one notification per minute. The Notifier MUST be capable of generating NOTIFYs at the maximum busy second call rate to the maximum number of downstream dequeueing entities, plus at least 10 other subscribers.

State Agents: Special handling is NOT REQUIRED.

Race conditions exist in which a dequeued call may be sent to an entity that just became congested. A call/event sent to a queue which is Inactive or Disabled, or in which the current queue length is equal to or greater than the allowed maximum queue length, will have a Status (486 Busy Here) returned by the dequeuer. An ESRP that dequeues a call, sends it to a downstream entity, and receives a 486 Busy Here in return, MUST continue evaluating the existing rule set per Section 3.3.3.2.1. Note that the upstream ESRP MAY be configured with policy rules that will specify alternate treatment based on downstream queue state.

ESRPs normally send calls to downstream entities that indicate they are available to take calls. "Available", however, is from the downstream entity's point of view. Network state

© Copyright 2011-2022 National Emergency Number Association, Inc.

may preclude an upstream entity from sending calls downstream. Normal SIP processing would eventually result in timeouts if calls were sent to an entity that never responds because the packets never arrive. Timeouts are long, however, and a more responsive mechanism is desirable to ensure that rapid response to changing network conditions route calls optimally.

If active calls are being handled, the upstream entity knows the downstream entity is connected. However, some routes are seldom used, and a mechanism MUST be provided that ensures the connectedness of each entity remains known.

For this purpose, relatively frequent NOTIFYs of the QueueState event are used. Successful completion of the NOTIFY is an indication to the upstream entity that calls sent to the downstream entity should succeed. The subscription may include a "force" and/or "throttle" filter (RFC 6446) [80] to control the rate of Notification.

4.2.1.4 DequeueRegistration Web Service

DequeueRegistration is a web service whereby the registering entity becomes one of the dequeueing entities, and the ESRP managing the queue will begin to send calls to it. Often, an ESRP or PSAP will manage a queue for which it is the only dequeuer; explicit DequeueRegistration for a single dequeuer is NOT REQUIRED. When there is more than one dequeuer, each dequeuer MUST register with this service. If the ESRP that manages the queue is also a dequeuer, it need not register (to itself). The registration includes a value for DequeuePreference that is an integer from 1-5. When dequeueing calls, the ESRP MUST send calls to the highest DequeuePreference entity available to take the call when it reaches the head of the queue. If more than one entity has the same DequeuePreference, the ESRP SHOULD fairly distribute calls to the set of entities with the same DequeuePreference measured over tens of minutes. The OpenAPI definition of this web service may be found in Appendix E.3. It contains one function:

HTTP method: PUT

Resource name .../Registration

A Registration object in the body of the PUT contains:

Name	Condition	Description
queueUri	MANDATORY	SIP URI of queue on which to register
dequeuerUri	MANDATORY	SIP URI of dequeuer (where to send calls)
expirationTime	MANDATORY	Requested time in seconds this registration will expire

© Copyright 2011-2022 National Emergency Number Association, Inc.

Name	Condition	Description
dequeuePreference	OPTIONAL	Integer from 1-5 indicating queuing preference.

A successful response returns expirationTime

Status Codes

200	OK
400	Bad Request
554	Unspecified Error
556	Bad queue
557	Bad dequeuePreference
558	Policy Violation

The expirationTime in the response is the actual expiration, which may be equal to or greater than that in the request depending on the local policy (DequeueExpirationTime) of the ESRP. A request expirationTime of zero is a request to deregister. The entity managing the queue has a policy (DequeueRegistration) of identifying which elements are permitted to register to be a dequeuer. The policy may include specific entities, or classes of entities, appropriate for the queue.

4.2.1.5 Policy Routing Function

Policy Routing refers to the determination of the next hop a call or event is forwarded to by an ESRP. The PRF evaluates one or more policy rule sets, whose syntax is described in Section 3.3.3: one set determined by the queue the call arrives on; a second may be determined by the result of an ECRF query with the location of the caller. One policy may invoke another policy.

The PRF in an ESRP accepts calls directed to a specific queue URI. (Any SIP URI that leads to an ESRP is considered a queue URI.) It extracts its own "RoutePolicy" from its Policy Store for that URI and executes the rule set. Usually at least one of the rules in the ruleset includes a condition LoSTServiceURN(<urn>) where <urn> is a service URN (either urn:service:… or urn:emergency:service:…). Upon encountering the LostServiceUrnCondition, the PRF queries its (configured) ECRF with the location received with the call using the <urn> parameter in the condition. If multiple location objects are presented with the call, the ESRP selects one, following the advice in Section 3.2 to be used for the ECRF query. If the query is successful, the resulting URI becomes the value of the variable "Normal-NextHop". The rule that has the LostServiceUrnCondition MUST contain an action "InvokePolicyAction" which uses the NormalNexthopRoutePolicy for

© Copyright 2011-2022 National Emergency Number Association, Inc.

<policyType>, and results in executing the rule set associated with the policy identified by the Normal-NextHop URI.

The destination of a Route action is the URI of a queue. The PRF has access to queue state of downstream entities and can use that state in evaluating rules. Rules normally have a Route action that sends the call to a queue that is available and not full. A Route may also be a URI that points to an Interactive Media Response system conforming to RFC 4240 [34], which plays an announcement (in the media negotiated by the caller) and potentially accepts responses via DTMF, KeyPress Markup Language (RFC 4730) [156], or other interaction styles.

Other Actions that may occur in a NormalNexthopRoutePolicy include Busy and Notify. By using these mechanisms, the full range of call treatments can be applied to any class of call for any circumstance based on the PRF rule set.

Rules have a priority. If more than one rule evaluates to true, the rule with the highest priority prevails.

Usually, there is a generic rule for use when everything is in normal status. Most calls will route via this rule, for example, "IF True THEN InvokePolicyAction(NormalNexthopRoutePolicy)". Other rules exist for unusual circumstances.

In congestion for typical transient overload, a specific PSAP would be delegated to take diverted calls (via a rule other than the generic rule). A call is said to be diverted when it is sent to a PSAP other than the one serving the location of the caller, usually due to some failure or overload condition. A queue may be established for that route, with one target PSAP. Such a diversion PSAP would be accepting calls on its normal queue as well as the diversion queue. Its rules can differentiate such calls from the queue on which they arrive.

For more extensive overload, a group of PSAPs would subscribe to take calls from a designated queue. For example, all PSAPs in neighboring counties might subscribe to a queue that has a low priority rule that enqueues calls to it for overload from a county PSAP. Similarly, all NG9-1-1 PSAPs in a state might dequeue for a "Denial of Service Attack" queue, or interstate queues may be established that have a "ripple" effect (using priority) to spread calls out when the state queue becomes busy. These queues are maintained by the ESRP. The ESRP dequeues a call from the queue on which it arrived, and enqueues it to the lower priority queue from which the multiple PSAPs will dequeue.

ESRPs managing a queue may receive calls from one or more upstream entities. Origination rules at the ESRP can govern how such calls are handled, as the URI used to get the call to the ESRP (which could be the name of a queue maintained at the ESRP) is an input to the PRF. When handling diverted calls, no ECRF dip may be needed. In such a

© Copyright 2011-2022 National Emergency Number Association, Inc.

case, the origination policy rule set would determine the route. PSAPs may dequeue for multiple call queues managed by it or other entities, placing them on internal queues for call takers.

4.2.1.6 ESRPnotify Event Package

The ESRP sends a Notify for this event when the PRF encounters a Notify action. It is used, for example, to inform entities that unusual conditions have occurred, and calls are being rerouted. The ESRPnotify event is defined as follows:

Event Package Name: emergency-ESRPnotify

Event Package Parameters:

Name	Condition	Description
NotifyEventQueueUri	MANDATORY	URI of queue that will contain a rule with a notify action
NotifyEventEventCodes	MANDATORY	Enumeration of event codes (see below). May occur more than once

SUBSCRIBE Bodies: Standard RFC 4661 [92] + extensions. Filter specification may be present

Subscription Duration: Default one (1) hour. One (1) minute to twenty-four (24) hours is reasonable.

NOTIFY Bodies: MIME type Application/EmergencyCallData.ESRProute+json

The content of the NOTIFY is contained in the table below.

ESRPnotify

Name	Condition	Description
queueUri	MANDATORY	URI of queue that Notify action occurred on
eventCode	MANDATORY	EventCode specified in Notify Action
urgency	MANDATORY	Urgency specified in Notify Action
comment	Conditional, MUST be present if Comment is specified in Notify action	Comment specified in Notify action
callLocation	MANDATORY	Location included with the call (by value or by reference as provided in the call)

© Copyright 2011-2022 National Emergency Number Association, Inc.

Name	Condition	Description
additionalData	Conditional, MUST be provided if AdditionalData is included with the call	Additional Data included with the call (by value or by reference as provided in the call), or retrieved using the Additional Data associated with a location mechanism, or from an IS-ADR.
esrpRule	MANDATORY	Rule that triggered the event

Note: If the URI in the Notify action in a rule contains a service URN, then the notification is sent to the entity whose service boundary intersects the location of the caller where the service URN matches that in the Notify action.

This document defines a registry, "EsrpNotifyEventCodes" which registers values that MAY be used in an <event code>. The initially defined values in the registry can be found in Section 10.19.

The NotifyBodiesEsrpCondition is a string consisting of the actual rule, per standardized syntax in Section 3.3.3.

Note: A future version of this document will describe how to include the condition values that triggered the notify in the body of the NOTIFY.

Notifier Processing of SUBSCRIBE Requests: The Notifier (the ESRP) consults the policy (NotifyPermissions) for Normal-NextHop to determine if the requester is permitted to subscribe. If not permitted, the ESRP returns 603 Decline. The ESRP determines whether at least one policy it uses contains a Notify action with that event code. If not, the ESRP returns a 488 Not Acceptable Here. If the request is acceptable, the ESRP returns 200 OK.

Notifier Generation of NOTIFY Requests: The <notify> action causes the ESRP to send NOTIFY to a set of entities, which have previously subscribed to the EventCode and queue. If the recipient value in the Notify action is present and contains one or more URIs, NOTIFYs are sent to all entities in the recipient list. If the recipient list contains a urn, NOTIFYs are sent to all subscribers whose service area contains at least a part of the call location and whose service URN matches the recipient value in the Notify action. If no recipients are included in the action, all subscribers for the EventCode are notified.

Subscriber Processing of NOTIFY Requests: No specific action required.

Handling of Forked Requests: Forking between elements MUST NOT be used.

Rate of Notification: A notification for each call/event handled by the ESRP could be sent. Rate controls (RFC 6446) [80] MAY be used to limit Notifications.

State Agents: No special handling is required.

© Copyright 2011-2022 National Emergency Number Association, Inc.

4.2.1.7 Processing of an INVITE or MESSAGE transaction

When the ESRP receives an INVITE transaction its PRF first evaluates the Origination rule set for the queue on which the call arrived. If the queue handles emergency calls, a LoSTServiceURN condition is normally encountered, which looks for the presence of a Geolocation header field. If present, the ESRP evaluates the header field and extracts the location following the URL found in the Geolocation header field (RFC 6442) [8]. Each ESRP MUST be capable of receiving location as a value or a reference and MUST be provisioned with credentials suitable to present to any LIS in its service area to be able to dereference a location reference using either SIP or HELD. For HELD location URIs, specifying a "responseTime" attribute set to "emergencyRouting" requests an immediate response with a location suitable for routing. For SIP location URIs, a SUBSCRIBE with an "Expires" header field set to 0 requests an immediate location response without creating a subscription. See Section 3.2 for guidance if multiple location objects are presented in the emergency call.

The ESRP MUST be able to handle emergency calls with problems in location. For example, this can occur if the emergency call has no Geolocation header field at all, or the Geolocation header field value is a "cid" URL pointing to an empty body part (i.e., the PIDF-LO is not present in the body). This can also occur if the location contents are malformed, the LIS cannot be contacted, the LIS refuses to dereference, the LIS returns a malformed location value, or the ESRP encounters another error that results in no usable location being available. In all such cases the ESRP MUST determine a suitable LVF-valid default location to use to route a call with location problems, as part of the LoSTServiceURN condition processing. In other words, the ESRP MUST ensure the pre-conditions as are always there for the LoSTServiceURN condition to be evaluated successfully. For example, the call source, the IP address of the caller, or other information from the INVITE MAY be used to determine the best possible default location. This procedure is based on the assumption that the earlier in call processing that bad or missing location is identified, the more likely it is that the ESRP will have the information needed to determine the best possible default location.

A PIDF-LO containing a Default Location MUST have its <method> element set to the value "Default"[22], and its <provided-by> element set to the identity of the NGCS provider

[22] The "Default" value must be registered in the Method Token registry with IANA. The Value is "Default" and the definition is "No location can be determined, or the location provided is unusable. A default location is used."

© Copyright 2011-2022 National Emergency Number Association, Inc.

that inserted it. The location elements MUST be populated to a level that yields an appropriate route URI in the LoST response from the ECRF.

- The ESRP SHALL perform the following procedures when handling a default location:The ESRP SHALL preserve the original Geolocation header field values and PIDF-LO documents in the original INVITE;
- If there is no Geolocation header field, the ESRP SHALL add the default location PIDF-LO document in the body of the INVITE (to do so, the ESRP MUST behave as a B2BUA), and add a Geolocation header field populated with a "cid" URI pointing to it;
- If there is a Geolocation header field value in the original INVITE (but no associated body part), a new one is created and placed as the top-most entry of the Geolocation field sequence;
- If the original INVITE contained a garbled PIDF-LO, the ESRP SHALL add a new body part with the default location PIDF-LO (to do so, the ESRP MUST behave as a B2BUA) and add a new Geolocation header field with a "cid" URI pointing to it as top-most entry of the Geolocation field sequence, retaining the garbled one;
- If the original INVITE contained a garbled location reference in the Geolocation header field, or the location dereferencing timed out or yielded a garbled PIDF-LO document, the ESRP SHALL add a new body part with the default location PIDF-LO document (to do so, the ESRP MUST behave as a B2BUA) and add a new Geolocation header field with a "cid" URI pointing to it as top-most entry of the Geolocation field sequence, retaining the garbled one;
- Once the INVITE has been groomed with a usable location for routing, albeit a default one, the ESRP MUST reprocess the Origination-Policy rule, including the LoSTServiceURN condition. Normal call processing ensued thereafter as described below.

The ESRP then queries its local (provisioned) ECRF with the location, using the service URN specified and in the LoSTServiceURN condition member. For example, an Originating ESRP receiving an emergency call from outside the ESInet, in an environment where there are no intermediary ESRPs in its service area (meaning the originating ESRP routes calls directly to the PSAP), may use the service "urn:emergency:service.sos.psap". The ECRF returns a URI for that service. If the ESRP receives an error indication from the ECRF, or the ESRP does not receive a response from the ECRF within a specified period of time, the LostServiceUrn condition evaluates as 'false'; evaluation of the ruleset conditions continues. If all rules fail then the ESRP MUST invoke the Fatal Error ruleset (see section 4.2.1.6).

Any rule set may include an "InvokePolicy" action. Originating rule sets will always have at least one InvokePolicy action for the Normal-NextHop URI. The PRF evaluates the rule set specified in the InvokePolicy action. The ruleset typically has rules that test information

© Copyright 2011-2022 National Emergency Number Association, Inc.

available at the ECRF (such as PSAP state, time of day, queue state, information extracted from the INVITE, etc.) The ruleset may transfer control to another ruleset. The final ruleset normally has a terminal action such as RouteAction, which causes the ESRP to attempt to forward the call to a queue URI, using the DNS to translate the URI into an IP address. If a default location is used to determine the route for the emergency call, the ESRP SHALL pass the location information received in incoming signaling forward in the outgoing SIP INVITE/MESSAGE.

DNS MAY provide alternate IP addresses to resolve the URI determined by the ESRP. Normal SIP and DNS processing is used to try these alternate IP addresses. Should no entity respond, the ESRP MUST reevaluate the ruleset with the rule which failed, interpreted as not satisfying its conditions.

Calls to an administrative number are recognized by the value in the To header. Administrative calls do not have location, so they MUST be routed using a provisioned table in the ESRP that associates the called number or sip URI to a URI of a queue in the ESRP.

Calls that are received by an ESRP which originate inside the ESInet (acting as a default outbound proxy) are routed per normal SIP routing mechanisms. Calls destined outside the ESInet are routed to the OCIF.

4.2.1.8 Processing a BYE Transaction

An ESRP MUST process BYEs per RFC 3261 [10].

4.2.1.9 Processing a CANCEL transaction

An ESRP MUST process CANCELs per RFC 3261.

If a call arrives at the ESRP but a CANCEL is received prior to any round trip from a PSAP, such that the ESRP is unsure whether the PSAP ever got an INVITE, it SHOULD notify the PSAP using the AbandonedCall event.

4.2.1.10 Processing an OPTIONS transaction

An ESRP MUST process OPTIONS transactions per RFC 3261 [10]. OPTIONS is often used as a "keep alive" mechanism. During periods of inactivity, the ESRP SHOULD periodically send OPTIONS towards its downstream entities and expect to see OPTIONS transactions from its upstream entities. If the downstream entity is not reachable, the ESRP MUST treat its queues as Inactive.

© Copyright 2011-2022 National Emergency Number Association, Inc.

4.2.2 Interface Description

4.2.2.1 Upstream Call Interface

The ESRP has an upstream SIP interface that typically faces a BCF for the originating ESRP or an upstream ESRP for an intermediate or terminating ESRP. This interface also is used by a PSAP for calls it originates over the ESInet. The upstream SIP call interface for the originating ESRP must only assume the minimal methods and header fields as defined in Section 3.1.1, but MUST handle any valid SIP transaction. All other ESRPs MUST handle all methods and SIP header fields. The ESRP MUST respond to the URI returned by the ECRF and/or specified in a Route action for a rule for the upstream service the ESRP receives calls from.

The upstream SIP interface is also used for calls originated inside the ESInet, where the ESRP is the outgoing proxy for a PSAP it serves. Non-emergency calls originated within the ESInet are routed to the OCIF.

The upstream interface on the originating ESRP MUST support UDP, TCP, and TCP/TLS and MAY support SCTP transports. The upstream interface on other ESRPs MUST implement TCP/TLS but MUST be capable of fallback to UDP. SCTP support is OPTIONAL. The ESRP SHOULD maintain persistent TCP and TLS connections to downstream ESRPs or UAs that it serves.

4.2.2.2 Downstream Call Interface

The ESRP downstream call interface typically faces a downstream ESRP for all but the terminating ESRP, which typically faces a PSAP's Call Handling FE. The downstream SIP call interface MUST implement all SIP methods to be able to propagate any method invoked on the upstream call interface. The downstream interface MAY add any header fields noted in Section 3.1.5 permitted by the relevant RFCs to be added by proxy servers. The INVITE transaction exiting the ESRP MUST include a Via header field specifying the ESRP. It MUST include a Route header field containing a URI (which should contain the "lr" parameter to avoid Request-URI rewriting) of the downstream queue that receives the call. The Request-URI remains "urn:service:sos"[23] (although the ESRP may not depend on that; a call presented to an ESRP that is not recognized as an emergency call, for example, a call to an admin line, MUST be treated as an emergency call and its occurrence logged) and it replaces the top Route header field with the next hop URI (this is described in RFC 6881

[23] The request URI does not change in the outgoing SIP message, even though the service URN used to query the ECRF may not be urn:service.sos. This is done through loose routing as defined in RFC 3261 [10] where the "lr" parameter is present in URIs used for routing.

© Copyright 2011-2022 National Emergency Number Association, Inc.

[46]). The ESRP adds History-Info header field and Reason parameter header fields per Section 3.1.8 using the cause code specified in the Route action if cause is specified (which would always be the case for a diverted call).

A call entering the ESInet is initially assumed to be a new Incident. Thus, the first ESRP in the path MUST add a Call-Info header field, if one is not already present, with a purpose parameter of "emergency-IncidentId" and a new Incident Tracking Identifier per Section 2.1.7. The ESRP MUST also create a new Call identifier (Section 2.1.6) and add a Call-Info header field with a purpose parameter of "emergency-CallId" if one is not already present. For example:

```
Call-Info: <urn:emergency:uid:incidentid:a56e556d871:bcf.state.pa.us>;
purpose=emergency-IncidentId
Call-Info: <urn:emergency:uid:callid:a56e556d871:bcf.state.pa.us>;
purpose=emergency-CallId
```

The downstream interface MUST implement TCP/TLS towards downstream elements but MUST be capable of fallback to UDP. SCTP support is OPTIONAL. An ESRP MAY NOT remove header fields received in the upstream call interface; all header fields in the upstream message MUST be copied to the downstream interface except as required in the relevant RFCs. The ESRP SHOULD maintain persistent TCP and TLS connections to downstream ESRPs.

The downstream SIP interface MAY also accept calls originating within the ESInet, specifically for callback. A callback would be accepted on its downstream interface and sent towards the originating network on its upstream interface.

4.2.2.3 ECRF interface

The ESRP MUST implement a LoST interface towards a (provisioned) ECRF. The ESRP MUST use a TCP/TLS transport and MUST be provisioned with the credentials for the ECRF. The ESRP SHOULD maintain persistent TCP and TLS connections to the ECRF.

This document defines service URNs that can be used by an ESRP to query an ECRF. These service URNs include:

URN	Use
urn:emergency:service:sos.psap	Route calls to primary PSAP
urn:emergency:service:sos.level_2_esrp	Route calls to a second level ESRP (for example, a state ESRP routing towards a county ESRP)
urn:emergency:service:sos.level_3_esrp	Route calls to a third level ESRP (for example, a regional ESRP that received a call from a state ESRP and in turn routes towards a county ESRP).

© Copyright 2011-2022 National Emergency Number Association, Inc.

URN	Use
urn:emergency:service:sos.call_taker	Route calls to a call taker within a PSAP. Note that the call handling FE in the PSAP may handle this instead.

ESRPs use these service URNs to perform finer resolution routing (e.g., state to regional, regional to psap, or other next hop). Each ESRP in the path MAY use a different service URN that relates to the hierarchy of routing within a given ESInet. The URIs returned by the ECRF using these service URNs (along with location) would be associated with queues used by downstream elements. Typically, those queues would not allow any entity other than the upstream ESRP to enqueue calls on that queue, which is specified by that queue's policy (See Section 4.2.1.4). The specific service URN used by an ESRP is specified in its origination routing policy (see Section 3.3.3.1.9). Any URN in the "urn.service.sos" (and its urn:service:test.sos equivalents) or "urn:emergency.service.sos" tree MUST be supported by all ESRPs. Loops can result if the service urns specified in the policy are not appropriately chosen.

There are no other entities inside or outside the ESInet other than ESRPs (as described above) that use these specific emergency:service URNs; they normally would use "urn:service:sos". For example, a PSAP that manually corrects an erroneous location in a call that resulted in a misroute would use "urn:service:sos" to find the route to the correct PSAP, regardless of location.

The ESRP MUST use the ECRF interface with the "urn:emergency:service:additionaldata" service URN when accessing Additional Data associated with a location in the evaluation of a rule set that contains an Additional Data condition, as described in Section 4.2.2.5 Additional Data Interfaces. The same location used for the location-based route is used for the Additional Data query.

4.2.2.4 LIS Dereference Interface

The ESRP MUST implement both SIP Presence Event Package and HELD dereferencing interfaces. When the ESRP receives a location URI (in a Geolocation header field on the upstream SIP interface) it uses the LIS dereferencing interface to obtain a location value to use in its ECRF query. The ESRP uses its PCA-issued credentials to authenticate to the LIS[24]. The ESRP MUST use TCP/TLS for the LIS Dereferencing interface, with fallback to TCP (without TLS) on failure to establish a TLS connection. The ESRP SHOULD maintain

[24] The LIS must accept credentials issued to the ESRP traceable to the PCA. If a call is diverted to an alternate PSAP, it could be any willing PSAP, anywhere. The alternate PSAP must be able to retrieve location.

© Copyright 2011-2022 National Emergency Number Association, Inc.

persistent TCP and TLS connections to LISes with which it has frequent transactions. A suggested value for "frequent" is more than one transaction per day.

4.2.2.5 Additional Data Interfaces

The ESRP MUST implement mechanisms for retrieving Additional Data (RFC 7852) [107]. These services are invoked when the ESRP receives a call with a Call-Info (RFC 3261) [10] header field having a "purpose" starting with "EmergencyCallData" a dot, and a block name[25], or from a PIDF-LO with an appropriate <provided-by> element and when directed to do so by the invoked rule set. The resulting data structure is an input to the Policy Routing Function (PRF). The ESRP MUST be able to accommodate multiple additional data services and structures for the same call.

Additional Data, when passed by reference, is retrieved by dereferencing each provided URI against its associated Additional Data Repository (ADR).

Multiple Call-Info header fields (or one or more Call-Info header fields containing multiple values) with a "purpose" parameter prefix of "EmergencyCallData", a dot, and an Additional Data block name, passed by value using the Content Identifier or by reference with an HTTPS URI, may occur (e.g., when more than one originating network handles the call and/or the device itself reports data). For example, a call may have Additional Data provided by a wireless carrier as well as a telematics service provider or the device (see 3.1.19 for more information about telematics calls and datasets).

Additional Data is primarily accessed via the following mechanisms:

- Through dereferencing URI(s), added to a Call-Info header field by the device, originating network, or service provider handling the call. Additional Data can be passed by reference via an HTTPS URI (referencing an external ADR) and by value via a Content Identifier (CID) URI (referencing a body part). Each by-reference Additional Data URI is dereferenced against its respective target ADR to return an Additional Data block.
- By querying an "Identity Searchable Additional Data Repository" (IS-ADR) with the identity obtained from Caller's From or P-Asserted-Identity header fields to retrieve any available Additional Data[26] blocks.

Additional Data may also be retrieved by the ESRP through a location-based query executed against the ECRF. This query returns a URI for Additional Data associated with

---

[25] e.g., purpose=EmergencyCallData.ProviderInfo

[26] Refer to Section 4.11.1 Identity Searchable Additional Data Repository (IS-ADR) for further detail on the interfaces exposed by this functional element.

© Copyright 2011-2022 National Emergency Number Association, Inc.

that location. This URI is dereferenced by the ESRP against an ADR as needed by PRF rules. Any such returned Additional Data URI MAY be added in a Call-Info header field so that it can be more easily accessed by downstream systems. The location used for this query may specify an area that encompasses more than one location that has Additional Data. In that event, the ECRF returns more than one mapping, each with a URI. The ECRF is not expected to handle more than 100 mappings, and MAY truncate its response if more than 100 mappings would be returned from a query. A new warning is defined in Section 3.4.10.5 for this condition.

The call MAY have more than one of each block type of Additional Data. This can occur when, for example, the call is from a residence wireline telephony service in which there is more than one resident and each supplies its own Additional Data blocks or multiple service providers participate in the call. When used in a routing rule, the PRF merges multiple "like" Additional Data objects. If the merge results in conflicting information, the information identified as most recently updated by the data source shall take precedence over information determined to be older.

Note: Using the latest data may be problematic in some situations. Making the rules for merging objects more explicit would limit cases of conflicting information. This will be covered in a future version of this document.

When evaluating a rule set that contains an Additional Data condition, at minimum the ESRP accesses and evaluates against the condition criteria all Additional Data blocks that are conveyed by value or by reference via Call-Info header fields. It is implementation dependent if the ESRP also performs an ECRF query for URIs for Additional Data associated with a location and then dereferences those URIs, or queries IS-ADRs, to access and evaluate further Additional Data blocks against the Additional Data condition.

Note that when retrieving Additional Data from an ADR, an HTTP Redirect may occur, which may itself lead to a redirect, etc. ESRPs should protect against excessive delay when accessing Additional Data (e.g., using timers and/or maximum redirect counters). ESRPs log resulting error situations (using the AdditionalDataResponseEvent) and may generate Discrepancy Reports against the policy owner, and if feasible, the ADR operator.

4.2.2.6 ESRP, PSAP, and Call Taker State Notification and Subscriptions

The ESRP MUST implement the client side of the ElementState and ServiceState event notification packages. The ESRP MUST maintain Subscriptions for these packages on every downstream element/service it serves. These state interfaces supply inputs to the Policy Routing Function.

The ESRP MUST implement the server-side of the ElementState event notification package and accept Subscriptions for all upstream ESRPs from which it expects to receive calls. The

© Copyright 2011-2022 National Emergency Number Association, Inc.

ESRP MUST promptly report changes in its state to its subscribed elements. Any change in state that affects its ability to receive calls MUST be reported.

The set of ESRPs within an NGCS MUST implement the server-side of the ServiceState event notification package. It is RECOMMENDED that if there are multiple levels of ESInet within a state, that the state level NGCS implement ServiceState as a single service, rather than having a ServiceState for each level of NGCS within the state. In such a service, if any regional or local NGCS' ESRPs are not operating properly, the state ESRP service would show some form of non-normal state for the ESRP ServiceState.

4.2.2.7 Time Interface

The ESRP MUST maintain reliable time synchronization. The time-of-day information is an input to the Policy Routing Function as well as the logging interface.

4.2.2.8 Logging Interface

The ESRP MUST implement a logging interface per Section 4.12. The ESRP MUST be capable of logging every transaction and every message received and sent on its call interfaces, every query to the ECRF, and every state change it receives or sends. It MUST be capable of logging the rule set it consulted, the rules found to be relevant to the route, and the route decision it made. Specific LogEvent records for these are provided in Section 4.12.3.

4.2.2.9 AbandonedCall Event

The ESRP uses the AbandonedCallEvent to notify a PSAP that a call was started, but then cancelled prior to the PSAP responding to the INVITE. The AbandonedCall Notify is sent to the PSAP that would have received the call, had it been completed. If rule set evaluation was not complete when the call was abandoned, rule evaluation with best-effort values for conditions in the rules is completed in order to determine where to send the Notify.

Event Package Name: emergency-AbandonedCall

Event Package Parameters: None

SUBSCRIBE Bodies: Standard RFC 4661 [92] + extensions filter specification may be present

Subscription Duration: Default one (1) hour. One (1) minute to twenty-four (24) hours is reasonable.

NOTIFY Bodies: MIME type application/emergencyCallData.AbandonedCall+json

© Copyright 2011-2022 National Emergency Number Association, Inc.

Name	Condition	Description
invite	MANDATORY	Content of INVITE message
inviteTimestamp	MANDATORY	Timestamp call was received at ESRP
cancelTimestamp	MANDATORY	Timestamp CANCEL was received at ESRP

Notifier Processing of SUBSCRIBE Requests: The notifier consults the policy (AbandonedCall) to determine if the requester is permitted to subscribe. It returns 603 (Decline) if not acceptable. If the request is acceptable, it returns 200 OK.

Notifier Generation of NOTIFY Requests: When the ESRP receives a CANCEL for a call prior to any non-100 response received from a PSAP, such that the ESRP is unsure whether the downstream entity ever got an INVITE, a new NOTIFY is generated to the PSAP that would have received the call as determined by interpreting the ruleset, adhering to the filter requests. If there are multiple ESRPs in the path, the ESRPs before the terminating ESRP may not get the INVITE or the CANCEL, but will receive a NOTIFY from the upstream ESRP. They MUST send a NOTIFY downstream following the above process.

Subscriber Processing of NOTIFY Requests: No specific action required.

Handling of Forked Requests: Forking between elements MUST NOT be used.

Rate of Notification: A series of fast INVITE/CANCEL is a possible DDoS attack. The rate of notification SHOULD be limited to a provisioned value. Three (3) per second is a reasonable limit.

State Agents: No special handling is required.

4.2.2.10 Secure Telephone Identity Verification Service Interface

The ESRP has a SIP interface to the STI-VS FE (see section 4.21.1). The ESRP only invokes the STI-VS if an Identity header field value conforming to RFC 8224 [60] is received in incoming signaling. The ESRP MUST invoke the STI-VS before applying the RoutePolicy ruleset for the queue the emergency calls arrives on.

4.2.3 Policy Elements

The ESRP uses an RoutePolicy rule set for each queue it manages. The ESRP MUST have access to the appropriate RoutePolicy ruleset for every URI that the ECRF can return in response to a service query made by the ESRP (Normal-NextHop).

The enqueuer policy (Enqueuers) specifies which entities can enqueue calls on the queue.

© Copyright 2011-2022 National Emergency Number Association, Inc.

The ESRProuteEvent Policy determines which entities may subscribe to the ESRProute Event (see Section 4.2.1.6).

The QueueState policy determines which entities may subscribe to the QueueState event.

The ElementState policy determines which entities may subscribe to its ElementState event.

The ServiceState policy determines which entities may subscribe to its ServiceState event.

The DequeueRegistration policy determines which entities may subscribe to the DequeueRegistration event.

The ESRP MUST be provisioned with the policy store it uses. Use of an external Policy Store MUST be possible even if an implementation includes a Policy Store.

4.2.4 Provisioning

The ESRP is provisioned with:

- The queues it manages;
- The queues from which it dequeues;
- The default locations it uses, including (potentially) one for each origination domain, and an overall default location;
- The ECRF it uses;
- The Logging service it uses;
- Mappings from 10 digit PSAP telephone numbers to URIs (if the ESRP handles 10-digit calls on behalf of PSAPs);
- The Policy Store it uses;
- A maximum InvokePolicyAction counter value;
- A Fatal Error ruleset.

4.2.5 Roles and Responsibilities

An ESRP may be operated by a State, Regional, or local 9-1-1 Authority. Downstream entities maintaining queues that upstream ESRPs queue calls on MUST supply a rule set for the upstream ESRP.

4.2.6 Operational Considerations

A routing rule that dereferences Additional Data from a server that is not under the control of a 9 1 1 Authority could add significant delay when processing the rule, and could increase fragility (decrease reliability).

© Copyright 2011-2022 National Emergency Number Association, Inc.

4.2.6.1 Tactical NG9-1-1 Emergency Call Routing Changes

Tactical routing is defined as the alternate routing of calls on short notice due to an unforeseen situation. An example of such is when the footprint of a disaster is greater than previously envisioned; thus, the policies in the PRF were not designed for such a condition. Both the ECRF and the ESRP/PRF are involved in the routing of NG9-1-1 calls, leaving in question the best method of making spur-of-the-moment changes. Unfortunately, there is no clear-cut answer to this situation. The answer is highly dependent on a number of parameters, all of which are deployment-specific.

4.2.6.2 Making Changes In Policy Routing Rules

The PRF is the natural place to make changes to routing based on conditions at the time of the call. Changes made in PRR take effect on the very next call. Making the decision to make routing changes in PRR depends on a number of factors:

- Whether it is possible to construct a rule to detect the current condition;
- Ability and confidence in making routing rule changes on the fly;
- In the case routing rules are under service provider control, contractual agreements or other considerations might constrain making such changes;
- Ability to conduct test calls simulating the condition to validate the rule change.

4.2.6.3 Making Changes In the ECRF

When the nominal PSAP for a certain area is no longer available to take calls, the expected duration may warrant changing the nominal PSAP for the affected area(s). For example, calls to an urban PSAP may need to be distributed to a number of neighboring smaller PSAPs. An important consideration is that changes made in the ECRF may not take effect immediately, because responses to ECRF queries can be cached and reused as specified in the 'expires' field of the response. It is important to consider the following: the operational parameters of the ECRF that affect the 'expires' value; the operational processes involved in making changes to the ECRF; what value was configured in the ECRF; and the treatment calls will receive until such time that the changes fully take effect. It may be necessary to modify the policy rules to cover the interim period.

© Copyright 2011-2022 National Emergency Number Association, Inc.

4.3 Emergency Call Routing Function (ECRF) and Location Validation Function (LVF)

In i3, emergency calls are routed to the appropriate PSAP based on the location of the caller[27]. In addition, PSAPs may utilize the same routing functionality to determine how to direct emergency calls to the correct responder. The NG9-1-1 functional element responsible for providing routing information to the various querying entities is the Emergency Call Routing Function (ECRF).

The NENA NG9-1-1 solution MUST properly route incoming IP packet-based emergency calls to the appropriate or designated PSAP, as well as support the dispatch of responders to the right location. The location information used, when provided in civic form, MUST be proved sufficient for routing and dispatch prior to the call being placed. We refer to this as having a "valid" location for the call[28]. The i3 architecture defines a function called the LVF (Location Validation Function) for this purpose. The LVF is only used for civic location validation. There is no concept of validation of a geodetic location in LoST (5222) [48]. The primary validation is accomplished as locations are placed in a LIS during provisioning. Validation MAY also be done by an endpoint if it is manually configured with location, or if it retrieves location from the LIS (via a location configuration protocol (RFC 6443) [4]). LVFs MUST support draft-ecrit-lost-planned-changes [178] allowing a LIS to be notified of planned changes in GIS data and for it to pre-validate a location against this new GIS data before it becomes live. Periodic re-validation of stored location is also RECOMMENDED (RFC 6881) [46][29] [30].

---

[27] When coarse location is provided in a wireless call, the location is one agreed to between the wireless operator and the 9-1-1 Authority, and not the location of the caller, and thus the route will be to the designated PSAP.

[28] We note that RFC5222, which describes the LoST protocol used by the LVF, validates against the service urn provided in the query, which for an outside (the ESInet) entity would be urn:service:sos. Strictly speaking, this is a call routing validation. NG9-1-1 requires validation for dispatch purposes. The LVF will validate to a level suitable for both routing and dispatch when the urn:service:sos is specified in the query.

[29] Short periods (days or a few weeks) allow errors that arise due to changes in underlying data the LVF uses to validate to show up sooner. However, the more often a LIS validates, the more load this places on the LIS and the LVF. A maximum period of 30 days is recommended. LIS operators may wish to consult with the LVF operator to determine an optimal revalidation period.

[30] In areas that have little change in data, such as fully built out, stable communities that are already part of a municipality, it may be reasonable to set revalidation periods of 6 months or longer, especially if the lost-planned-changes [178] mechanism is widely used by LISes. In areas that are quickly growing, 20- to 30-day revalidation may be more appropriate even though such revalidation would be the majority of the traffic on the LVF.

© Copyright 2011-2022 National Emergency Number Association, Inc.

As specified in Section 3.4.2, the LVF MUST support the validation of location around planned changes as defined by draft-ecrit-lost-planned-changes [178].

ECRFs and LVFs are queried using the LoST protocol (see Section 3.4). 9-1-1 Authorities provide authoritative ECRFs and LVFs both inside and outside ESInets. Other entities, such as originating networks, can provide their own ECRF/LVFs, or equivalent functions that can be provisioned from authoritative data provided by the 9-1-1 Authority.

An ECRF or LVF provided by a 9-1-1 Authority and accessible from outside the ESInet MUST permit querying by an IP client/endpoint, an IP routing proxy, a Legacy Network Gateway, and any other entity outside the ESInet. An ECRF or LVF accessible inside an ESInet MUST permit querying from any entity inside the ESInet. ECRF/LVFs provided by other entities may have their own policies on who may query them. An originating network MAY deploy an ECRF, or a similar function within its own network, to determine an appropriate route, equivalent to what would be determined by the authoritative ECRF provided by the 9-1-1 Authority, to the correct ESInet for the emergency call. The ECRF MUST be used within the ESInet to route calls to the correct PSAP, and by the PSAP to route calls to the correct responders.

4.3.1 Functional Description

The ECRF/LVF supports a mechanism by which location information (either civic address or geo-coordinates) and a Service URN serve as input to a mapping function that returns a URI used to route an emergency call toward the appropriate PSAP for the caller's location (for an ECRF) and validation information (for an LVF). In an ECRF, depending on the identity and credentials of the entity requesting the routing information, the response MAY identify the PSAP or an Emergency Service Routing Proxy (ESRP) that acts on behalf of the PSAP to provide final routing towards the PSAP. The same database used to route a call to the correct PSAP MAY also be used to subsequently route the call to the correct responder (e.g., to support selective transfer capabilities). Depending on the type of routing function requested, the response may identify a secondary agency. In addition, the ECRF provides the capability to retrieve other location related URIs, such as Additional Data URIs.

ECRF/LVFs are arranged in trees. The ECRF and LVF trees are separate. The Forest Guide contains entries for (nominally) state level ECRF/LVFs. State ECRF/LVFs MAY be authoritative for the entire state, or it MAY refer or recurse to regional or local ECRF/LVFs. In some areas, regional ECRF/LVFs MAY have copies of all of the region's information or MAY refer to local ECRF/LVFs. Entities MAY perform LoST server discovery (as described in RFC 5223 [131]) to find their local ECRF or MAY be provisioned with a LoST server address. They send queries to that ECRF. A LIS has a provisioned LVF. The local ECRF/LVF can either answer the query or will refer or recurse in the tree to an ECRF/LVF that will eventually lead to the correct response. When stressed, or under attack, the Forest Guide

© Copyright 2011-2022 National Emergency Number Association, Inc.

MAY selectively refuse queries from any entity, for example, ECRF/LVFs whose coverage regions are not stored in the National Forest Guide. For this reason, it is RECOMMENDED that entities querying using LoST use recursion. Entities MUST NOT bypass their local ECRF/LVF and query a National Forest Guide directly. A National Forest Guide MAY reject queries from other entities, for example, if it is overloaded. Not all areas will have state level ECRF/LVFs and some local or regional ECRFs MAY be listed as stand-alone trees in a National Forest Guide. By arranging ECRFs and LVFs in this manner, and since the National Forest Guide will contain listings for all trees globally, a query to a local ECRF/LVF will result in a correct response for any location.

ECRFs SHOULD return an 'expires' element with at least a minute of cacheable mappings. Implementors should note the text in Section 3.3.3.1.9 when 'NO-CACHE' is returned.

4.3.2 Interface Description

4.3.2.1 Routing Query Interface

The ECRF and LVF query interface implements the LoST (RFC 5222) [48] protocol as described in Section 3.4. When an ECRF receives a LoST query, it determines whether the query was received from an authenticated entity (e.g., an ESRP) and the type of service requested (i.e., emergency services). Authentication MUST apply to all entities that initiate queries to the ECRF within the ESInet. TLS is used by all ECRFs and LVFs within the ESInet, and credentials issued to the querying entity that are traceable to the PCA MUST be accepted. Devices and carriers outside the ESInet may not have credentials, TLS is not required, and the ECRF/LVF should assume a common public identity for such queries. Based on the service requested, the ECRF determines which URI is returned in the LoST response, which could be a URI of a PSAP or a downstream ESRP. The same database used to route a call to the correct PSAP may also be used to subsequently route the call to the correct responder (e.g., to support selective transfer capabilities).

The ECRF is provisioned with a service boundary layer containing one or more service boundary polygons (See Appendix C). Each of the polygons contains attributes that specify the service URN that the polygon applies to and the URL the ECRF should return if the proffered location is within the polygon. Conceptually, the ECRF geocodes the location if it is specified in civic form and intersects the location of the service with polygons that have the same URN as the proffered service URN. The ECRF returns the URL attribute of the service boundary matching the URN that contains the location.

If the proffered location is not specified as a point (i.e., the location in the query is a shape) and the shape intersects more than one service boundary with a given service URN, the ECRF response SHALL be the URI of the service boundary with the greatest area of overlap (with a tie-breaking policy for the case of equal area of overlap).

© Copyright 2011-2022 National Emergency Number Association, Inc.

If more than one service boundary for the same service URN at a given location exists in the ECRF, multiple <mapping> elements will be returned. The querier (e.g., a PSAP), MUST have local policy to determine how to handle the call. In some cases, the ECRF can use the identity of the querier, or a distinguished Service URN to return the URI of the correct agency. This condition only occurs for queries to an ECRF from within an ESInet. External queries will only return one (PSAP) URI. The ECRF is not expected to handle more than 100 mappings, and MAY truncate its response if more than 100 mappings would be returned from a query. A new warning for this purpose is described in Section 3.4.10.5.

LoST MAY return a service boundary in the response, see Section 4.3.3.3.

In the deployment strategy envisioned in this document, a query from outside an ESInet for "urn:service:sos" is mapped to state level ESInets, and thus state ESRPs. The boundary returned in such cases is a state boundary, or subset of it as described above. Neither ECRFs nor LVFs are required to return service boundaries.

When a query is performed using a service URN that contains a subservice (e.g., "urn:service:sos.police" or "urn:service:sos.ecall.automatic"), if the ECRF does not have a service boundary with an attribute for that exact service URN, it uses the closest matching service URN. Thus, a multi-level subservice may match a more general subservice (such as "urn:service:sos.ecall" for "urn:service:sos.ecall.automatic") or no subservice ("urn:service:sos" for any subservice). When a query is performed using a service URN that is "urn:service:test.sos" or a subservice, it matches "urn:service:sos" with the same subservices. This is how test calls are routed the same as non-test calls. (Because the Request-URI is preserved, the receiving PSAP knows a test call from a non-test call.)

4.3.2.2 Validation Interface

RFC 5222 [48] Section 8.4.2 states that the inclusion of location validation is optional, and subject to local policy. All LoST server implementations, deployed as an LVF, MUST support the inclusion of location validation information in the "findServiceResponse" message. ECRFs may receive a request to validate a location. The ECRF MAY:

- Not return any validation response
- Perform the validation and return the validation response
- Recur (or refer) to an LVF that can perform the validation[31]

[31] Recursion to an LVF may not be desirable since the LVF is not a real-time element.

© Copyright 2011-2022 National Emergency Number Association, Inc.

Local policy at the ECRF determines what the ECRF does, which MAY take into account load at the ECRF.

Local LVF policy is also responsible for determining which elements are given priority in determining which URI and which associated location data element tokens are deemed valid. Sometimes different data elements are in conflict with each other. As in the example message, the findServiceResponse message returns the Postal Code (value of 45054) as <invalid>, showing that the A1 & A3 (State & City) data elements in combination – in this case – are given preference over a Postal Code that doesn't exist. Whereas the decision to prefer real data to non-existent data makes good sense, it is possible to have cases in which all data elements are real, but not consistent with each other. In this case, local policy will determine which elements are used, and are shown as valid.

As specified in Section 3.4.2, the LVF MUST support the validation of location around planned changes as defined by draft-ecrit-lost-planned-changes [178].

4.3.2.3 Mapping Data Provisioning Interface

The ECRF/LVF's data source is geospatial information, specifically, a set of layers from one or more source Spatial Interfaces (SIs). An SI layer replication interface, as described in Section 3.6, is used to maintain copies of the required layers. Appendix B describes the layers needed by the ECRF/LVF. The ECRF/LVF is provisioned with the URI of the SI and the information necessary to identify the required layers. It has layers that define the locations (state/county/municipality/street/address), as well as service boundary polygons. ECRF/LVFs may be built to coalesce data from more than one SI.

It is essential to the proper operation of the Next Generation 9-1-1 system that provisioning of the routing data in an ECRF is online, near real-time. An authorized change in the authoritative GIS to flow through the SI to the ECRF in near real-time is desirable, and SHOULD result in changes in routing immediately, although caching of mappings may prevent route changes from being honored as quickly. LVF provisioning is less critical.

4.3.2.4 Time Interface

The ECRF/LVF MUST implement an NTP client interface for time of day information. The ECRF/LVF MAY also provide an interface to a hardware clock. The time-of-day information is an input to the mapping expiration time as well as the logging interface.

4.3.2.5 Logging Interface

The ECRF/LVF MUST be capable of generating LogEvents per Section 4.12. The ECRF/LVF MUST be capable of logging every incoming routing/validation request along with every recursive request and all response messages. In addition, the ECRF/LVF MUST log all

© Copyright 2011-2022 National Emergency Number Association, Inc.

provisioning and synchronization messages and actions. Specific LogEvent records for these are provided in Section 4.12.3.

4.3.2.6 Element State

Each ECRF and each LVF MUST implement the server-side of the ElementState event notification package. The ECRF/LVF MUST promptly report changes in its state to its subscribed elements. Any change in state that affects its ability to route (ECRF) or validate (LVF) MUST be reported.

4.3.2.7 Service State

The set of ECRF and LVF FEs within an ESInet MUST implement the server side of the ServiceState event notification package for the ECRF and the LVF service. It is RECOMMENDED that if there are multiple levels of ESInet within a state, that the state level NGCS implement ServiceState as a single service, rather than having a ServiceState for each level of NGCS within the state. In such a service, if any regional or local NGCS' ECRF or LVF is not operating properly, the state ECRF and/or LVF service would show some form of non-normal state for the ECRF/LVF ServiceState.

4.3.3 Data Structures

4.3.3.1 Data to Support Routing Based on Civic Location Information

The ECRF MUST be able to provide routing information based on location information represented by a civic address. To do so, it is expected that the ECRF will represent the geographic service boundary in a manner that allows the association of a given address with the service boundary within which it is located. Theoretically, the ECRF maintains the civic address data as the SI layers used to provision it, using a geocode followed by point-in-polygon algorithms to determine the service boundary the civic address is located within. The ECRF MAY internally compute a tabular civic address form of data representation with the associated URI resulting from the point-in-polygon operation. This would reduce the LoST query resolution for a civic address to a table lookup. However, if the provisioning data changes, the ECRF MUST respond immediately to the change, which may invalidate (for at least some time) the precalculated tabular data.

ECRFs MUST accept location information conforming to U.S. addressing standards defined/ in CLDXF [77] and its eventual Canadian equivalents.

4.3.3.2 URNs

An ECRF/LVF MAY be authoritative for a given (set of) URN(s) in a given service area if they are provisioned from the authoritative SI for that area. There MAY be replicas of the

© Copyright 2011-2022 National Emergency Number Association, Inc.

ECRF/LVF, but they all supply the same resultant URI. ECRF/LVFs can recur or iteratively refer to other ECRF/LVFs or the National Forest Guide to obtain answers based on queries for service URNs or locations outside their area. Two queries from the same entity that uses the same service URN and location that are sent to different ECRFs SHOULD return the same response. Unless the ECRF/LVF is provisioned to return different responses to different credentials of the querier, all queries with the same URN and location SHALL return the same response.

4.3.3.3 Service Boundaries

The service boundary in a <mapping> MAY be returned by value or by reference, or not at all, at the discretion of the server. If the server returns a service boundary reference, the client may then obtain the actual service boundary with a <getServiceBoundary> request. A service boundary represented by a given reference can never change, so a client only needs to retrieve the boundary value a single time. Future mappings returned by the server and having the same service boundary MAY reuse the reference, eliminating the need to transmit the boundary value again.

Devices handling service boundaries may be limited in processing power and battery capacity, and thus sending complex polygons SHOULD be avoided. Devices may have to handle a polygon with several points when the device is very close to an edge where the mapping will be different. When a device is not close to an edge, a simplified representation of a geodetic service boundary (such as a simple shape that does not extend past the actual service area) SHOULD be returned.

Because a service boundary is not needed to initiate an emergency call an ECRF MAY be configured to return geodetic service boundaries by reference. Devices querying an ECRF in order to immediately initiate an emergency call SHOULD NOT attempt to obtain the service boundary by value.

As long as a device stays within the boundary returned, and is within the expiration time of the mapping, it need not re-query the ECRF.

Location represented by geodetic coordinates provides data that corresponds to a specific geographic location shape. A service boundary is represented by a polygon set. More than one polygon MAY occur in the set, for example, when the service area has holes or non-contiguous regions.

© Copyright 2011-2022 National Emergency Number Association, Inc.

For each service URN supported by an ECRF/LVF, one or more layers will provide polygon sets associated with URIs[32]. Two types of attribute are associated with these polygons:

- URN: The service URN this boundary is associated with
- URI: A URI returned if the location is within the boundary

The ECRF/LVF computes a response to a LoST query by finding the polygon whose service URN attribute matches that provided in the LoST query and whose service boundary contains the location provided in the LoST query, and returns the URI attribute of that polygon set. If the proffered location is a shape, that shape MAY overlap more than one service boundary. The ECRF response SHALL be the service boundary with the greatest area of overlap. The ECRF will return multiple <mapping> elements in a response if the query has multiple matches (e.g., a query within an ESInet for "emergency:service:responder:police" with a location within the jurisdiction of campus, city, county, and state police agencies) A querier could use the service boundaries (e.g., to determine which has the smallest service area and thus might be the most specific to the location).

Note that the provisioning interface to the ECRF/LVF is the SI layer replication protocol, and thus always delivers a geodetic service boundary definition to it. The ECRF/LVF MAY compute a civic representation of the boundaries internally. A trivial example is a service boundary polygon exactly matching a state, county, or municipal boundary.

4.3.3.4 Service to access Additional Data for a location

In the case of the Additional Data service, the ECRF does not use the service boundary polygons. Additional Data is associated with a site/structure. This will be addressed in a future version of this document. When the ECRF receives a findService request for the Additional Data service URN, and the proffered location information is a civic address, the ECRF returns the content of the Additional Data URI element associated with the site/structure, if available. If the location information proffered is a point, the ECRF finds the enclosing site/structure polygon, if there is one, or the nearest site/structure feature, and returns the associated Additional Data URI, if available[33]. In the case in which a location is a shape, rather than a point, and there are more than one site/structures

[32] Multiple URIs, each with a different scheme, may be returned from an ECRF query

[33] The Additional Data block is intended to reference the civic address to which it refers, so a geodetic querier can determine to which address the response refers. This will be addressed in a future version of this document.

© Copyright 2011-2022 National Emergency Number Association, Inc.

partially or completely within that shape, the ECRF returns all of the Additional Data URIs associated with those sites/structures[34].

When dereferenced by a client using PCA-traceable credentials, URIs returned for the Additional Data service MUST resolve to Additional Data blocks registered in the IANA Emergency Call Additional Data registry [179].

4.3.3.5 Routing Data – URI Format

For an end-to-end IP network in which the caller is an IP endpoint and the PSAP is accessed over an IP network, routing information will be in the form of a URI. The source of the query and/or the service URN determines which URI is returned. URI format is described in RFC 3986 [126]. URIs can be of variable length. It is suggested that the length allowed for a URI be as compact as possible, not exceeding 1.3 KB, which is the maximum size of a packet on the ESInet, less any header field information.

4.3.3.6 Validation Data

The LVF uses the same data provided to the ECRF as described in Section 4.3.3.1 above.

4.3.4 Coalescing Data and Gap/Overlap Processing

ECRFs and LVFs MAY coalesce data from several 9-1-1 Authorities. The resulting database appears to be a seamless route database for the union of the service areas of each 9-1-1 authority. Such ECRF/LVFs are provisioned to accept data from multiple GIS' via separate SIs.

In some local GIS', for convenience, the 9-1-1 Authority may provide data that extends beyond the service boundary of the PSAPs within their jurisdiction. When provisioning data for an ECRF and LVF through the SI, a 9-1-1 Authority (or 9-1-1 Authority designee) MUST only include GIS data for their geographic area of responsibility and MUST ensure the data includes coverage for the entire extent of that area. When the data are coalesced, boundaries may have gaps and overlaps. The relevant 9-1-1 Authorities SHOULD endeavor to address such issues early, but despite best efforts, the ECRF/LVF may encounter a gap or overlap. The ECRF/LVF MUST have a provisionable threshold parameter that indicates the maximum gap/overlap that is ignored by it. This threshold is expressed in square

[34] The definition of "nearest", when the ECRF is determining the Additional Data URIs from a point, is implementation-dependent. The querier can control this by sending a circle shape rather than a point, in which case the ECRF will intersect the circle with the site/structure entries, and return all of them that are completely or partially in the circle.If the number of URIs to be returned is large, the number of mappings in the response may be limited in an implementation-dependent way

© Copyright 2011-2022 National Emergency Number Association, Inc.

meters. Gaps or overlaps that are smaller than this parameter MUST be handled by the ECRF/LVF using an algorithm of its choice. For example, it may split the gap/overlap roughly in half and consider the halves as belonging to one of the constituent sources.

The ECRF/LVF MUST report gaps and overlaps larger than the provisioned threshold. To do so, it makes use of the GapOverlap event. All 9-1-1 Authorities which provide source GIS data to an ECRF/LVF MUST subscribe to its GapOverlap event. The event notifies all impacted agencies when it receives data that show a gap or overlap larger than the threshold. The notification includes the layer(s) in which the gap/overlap occurs, whether it is a gap or an overlap, and a polygon that represents the gap or overlap area. The optional effective and expires times in the data may indicate a future gap/overlap as opposed to one that exists when the event is generated. The report includes a Timestamp of when the gap/overlap will occur.

The response of the agencies MUST be to provide updates to the data that address the gap/overlap. The ECRF/LVF will repeat the notification at least daily until it is resolved (by changing the SI data so the gap/overlap is eliminated or at least smaller than the threshold parameter). During the period when the gap/overlap exists, notifications have been issued, and queries arrive (which could be at call time) with a location in the gap/overlap, the ECRF/LVF MUST resolve the query using an algorithm of its choice. For example, it may split the gap/overlap roughly in half and consider the halves as belonging to one of the constituent sources.

A service may have areas within the service area of the ECRF for which there is no responder. For example, the mountain rescue service is not available in flat terrain. Also, there are still some areas where 9-1-1 service is not available. In such cases, a service boundary MUST exist in the ECRF with the Service URI field set to urn:emergency:servicenotimplemented. The ECRF MUST return the <serviceNotImplemented> error if asked to provide a route for a location within that areas.

The GapOverlap event is defined as follows:

Event Package Name: emergency-GapOverlap

Event Package Parameters: none

SUBSCRIBE Bodies: Standard RFC 4661 [92] + extensions filter specification may be present

Subscription Duration: Default 24 hour. 1 hour to 96 hours is reasonable.

NOTIFY Bodies: MIME type Application/EmergencyCallData.GapOverlap+json

© Copyright 2011-2022 National Emergency Number Association, Inc.

Name	Condition	Description
agency	MANDATORY	URI of Agency with gap/overlap. Will be repeated at least twice
layer	MANDATORY	Enumeration of layer in which gap/overlap exists. May occur multiple times
gap	MANDATORY	Boolean: True if gap, False if overlap
dateTime	OPTIONAL	Timestamp when gap/overlap will occur. If not provided, gap/overlap is present now
area	MANDATORY	GML Polygon area of gap/overlap

Notifier Processing of SUBSCRIBE Requests: The Notifier consults the policy (NotifyPermissions) for GapOverlap to determine if the requester is permitted to subscribe; agencies allowed to provide authoritative data to the ECRF are permitted by default. If the requester is not permitted, the Notifier returns 603 Decline. Otherwise, the Notifier returns 200 OK.

Notifier Generation of NOTIFY Requests: When the provisioning GIS data creates a gap or overlap whose area is above the GapOverlapThreshold parameter, the Notifier generates a Notify to all subscribers. The Notifier repeats the Notification at least once per 24 hours as long as the gap/overlap remains.

Subscriber Processing of NOTIFY Requests: No specific action required.

Handling of Forked Requests: Forking between elements MUST NOT be used.

Rate of Notification: Notifies normally only occur when the provisioning data changes. Throttle MAY be used to limit Notifications.

State Agents: No special handling is required.

4.3.5 Replicas

An ECRF/LVF is essentially a replica of a subset of the layers of one or more source GIS' The ECRF/LVF in turn, may provide a feed to other ECRF/LVFs who wish to maintain a copy of its data. As the ECRF/LVF is not the data owner, the source GIS MUST have a policy (GISReplicas) that permits the ECRF/LVF to do so, and the policy MAY restrict to which entities it may provide replication data. The ECRF/LVF also has a policy (ECRF-LVFreplica) that defines to whom it will provide data. If the ECRF/LVF provides a replica service, the interface is the layer replication service as described in Section 3.6. In this case, the

© Copyright 2011-2022 National Emergency Number Association, Inc.

ECRF/LVF is the server-side, as opposed to the client interface it must provide towards the SI(s) from which it receives data.

4.3.6 Provisioning

The ECRF/LVF is provisioned with a set of layers from one or more SIs, the domains from which it may accept queries, if its use is restricted is specified with a policy (AcceptableLoSTQuerySources).

To maximize the probability of getting help for any kind of emergency to foreign visitors who may have separate dial strings for different types of emergencies, the ECRF/LVF SHOULD be provisioned with every sos URN in the IANA registry[35]. All sos service URNs that represent services provided by the PSAP return the dial string '911' and the PSAP URI. Other services available in the area would typically return a tel URI with the proper PSTN telephone number, other dial strings, or other provisioned values. In such cases, the telephone number for the service would also be returned in the service number parameter of the response. Any ECRF that is authoritative for a top level URN MUST also be authoritative for all lower level URNs for the same coverage regions.

4.3.7 Roles and Responsibilities

The ECRF/LVF plays a critical role in the location-based routing of emergency calls. Therefore, it is crucial that the data in the ECRF/LVF be accurate and authorized. 9-1-1 Authorities are responsible for providing the authoritative data for their jurisdiction to the ECRF/LVF. The data may be aggregated at a regional or state level, and the ECRF/LVF system provided at that level may be the responsibility of the associated state or regional emergency communications agency. In addition, access or originating network operators may maintain replicas of the ECRF/LVF. Thus, the operation and maintenance of individual ECRF/LVFs may be the responsibility of the provider of the network in which they physically reside, but it is the 9-1-1 Authority that is responsible for maintaining the integrity of the source data housed within those systems. The 9-1-1 Authority will also provide input to the definition of the policy which dictates the granularity of the routing data returned by the ECRF (i.e., ESRP URIs vs. PSAP URIs), based on the identity of the query originator and/or service URN.

[35] While there is only one dial string, 911, for emergencies in North America, all services in the sos tree should return a valid route when queried. For services the PSAP is responsible for, such as sos.police, the same URI used for urn:service:sos should be returned.

© Copyright 2011-2022 National Emergency Number Association, Inc.

4.3.8 Operational Considerations

The NG9-1-1 architecture allows for a hierarchy of ESInets, with replicas of ECRF/LVFs at different levels of the hierarchy as well as in access/originating networks. It is expected that ECRFs that are provided as local copies to network operators will only have the layers necessary to route to the correct originating ESRP, whereas ECRFs that are inside the ESInet(s) will have all available layers and use authorization to control who has access to what information. Since it is not possible that all entities that need to access an ECRF will have one in their local domain, an ECRF for each 9-1-1 Authority MUST be accessible from the Internet[36]. Consideration needs to be given to the operational impacts of maintaining different levels of data in the various copies of the ECRF. In addition, tradeoffs between the aggregations of data in higher level ECRFs versus the use of Forest Guides to refer requests between ECRFs that possess different levels of ECRF data must be considered. LVFs always provide the same data to all queriers and thus are provisioned identically. Provisioning of data within appropriate ECRF/LVF systems for use in overload and backup routing scenarios MUST also be supported.

For example, a local ECRF may have an SI to another local ECRF, a regional ECRF may have an SI to all the local ECRFs in its area, a state ECRF may have an SI to all of the regional ECRFs, and an access network provider may have an ECRF that has an SI from the state ECRF. A change in the GIS system by the local 9-1-1 Authority is propagated via its local SI to the local ECRF, and that local ECRF propagates it to the regional ECRF, which propagates it to the state ECRF that propagates it to the access network ECRF.

The placement of ECRF/LVF elements in the IP-enabled network varies with implementation. Since both end devices as well as LIS elements need to validate location, it is recommended that LVF elements are within the local domain or adjacent to it. Given that NG9-1-1 elements will also need to validate civic locations that either come with an emergency call, or are conveyed over the voice path, it is also a requirement that LVF elements MUST be reachable from within any ESInet. Since it is not possible that all entities that need to access an LVF will have one in their local domain, an LVF MUST be accessible from the Internet[37]. Similar considerations apply for an ECRF, but the entities that route are often different from the entities that validate, so differences in deployments may occur. All devices and services that route MUST have access to an ECRF. External ECRFs MUST be accessible to all devices and services, including those on the Internet.

---

[36] The Internet-accessible ECRF may be a state or regional ECRF containing the local ECRF data of all 9-1-1 Authorities within the state or region.

[37] The Internet-accessible ECRF/LVF may be a state or regional ECRF/LVF containing the local data of all PSAPs within the state or region.

© Copyright 2011-2022 National Emergency Number Association, Inc.

Ideally, originating networks will have replicas of the authoritative (usually state) ECRFs maintained inside their networks for use by their services and devices. Within the ESInet, ECRFs MUST be accessible from all ESRPs and all agencies that may receive or transfer calls or EIDOs related to calls.

LVF elements are based on the LoST server architecture and use the LoST protocol (RFC 5222) [48]. The LVF is a logical function that MAY share the physical platform of an ECRF, and MUST share the same data for a given jurisdiction as the ECRF. The justification for shared data is rooted in the idea of consistency – expecting a similar result from the same, or matching data. The LVF is used during a provisioning process (loading data into a LIS for example), while an ECRF is in the near real-time call flow. Separating the functions may make more sense. The Service Level Agreements for the two functions may dictate whether they can be combined or not.

An ECRF/LVF, wherever deployed, whether within an Origination or Access network, MUST be able to reach out to other ECRF/LVFs in case of missing data, or in the case in which the requested location is outside its local jurisdiction. If the ECRF/LVF doesn't know the answer, based on configuration, it will either recurse (refer) a request for validation to one or more other ECRF/LVFs, or it will iterate the request to some other ECRF/LVF, providing the other ECRF/LVF's URL in the original ECRF/LVF response.

Redundant ECRF/LVF elements are RECOMMENDED, similar to DNS server deployments (the ECRF/LVF shares some of the same replication characteristics with DNS), by example, in order to maintain a high level of availability and transaction performance.

Given the close association between the LVF and ECRF elements, ECRF/LVFs SHOULD be deployed hierarchically and with "n" number of replicas at each level of the hierarchy. The same redundancy/replica considerations apply to access/calling/originating networks that use an ECRF/LVF. This level of redundancy aids in maintaining high levels of availability during unexpected system outages, scheduled maintenance windows, data backup intervals, etc.

Localized ECRF/LVF elements MAY have limited data, sufficient to provide routing/location validation within its defined boundaries, but MUST rely on other ECRF/LVFs for routing/validation of a location outside its local area.

ECRFs and LVFs within the ESInet will likely have considerably more data than those in access or originating networks, providing aggregation for many local access areas as well as PSAP jurisdictions. Even the level of data that an ECRF/LVF might contain will vary depending on the hierarchy of the ESInet that it supports. An ESInet serving a local PSAP MAY have within its ECRF/LVF only base civic location data for its described jurisdiction, whereas a State-level or County-level ECRF/LVF MAY aggregate all of the local PSAP data within that level of hierarchy.

© Copyright 2011-2022 National Emergency Number Association, Inc.

Tactical Routing considerations in NG9-1-1 may require an Emergency Call Routing Change made in the ECRF. See discussion of ECRF changes in Section 4.2.6.3.

4.3.9 Internal and External ECRF/LVFs

ECRF/LVFs exist inside and outside the ESInet. Originating networks that route calls to the correct ESInet and validate locations MAY use external ECRFs. Originating networks MAY also use equivalent mechanisms that would result in the same route that the external ECRF would provide for the location of the caller for a querier without credentials known by the ECRF. Internal ECRF/LVFs are used by elements inside the ESInet to route calls to the appropriate downstream entity and validate civic locations. While the interfaces and functional descriptions are nearly identical, the provisioning data may not be the same for internal and external ECRFs. An external ECRF need only have the external (which ESInet) route for "urn:service:sos.*" The internal ECRF also needs routes for ESRP use ("urn:emergency:service:sos.*") and other internal services such as "urn:emergency:service:serviceagencylocator". If the data in the internal and external ECRFs are different, this would only affect service boundary data. All LVFs are provisioned with the same data, whether inside or outside the ESInet.

4.3.10 Relationship Between ECRF and LVF

The ECRF and LVF functions have the same interfaces and contain the same data. They MAY be combined into a single implementation. However, it should be noted that the ECRF is a real-time element in the path of an emergency call. The LVF is used primarily while provisioning a LIS. If the ECRF and LVF are combined, the implementation MUST assure ECRF queries are processed promptly, and LVF traffic does not interfere with proper operation of the ECRF function.

LVF interaction at emergency call time MAY be performed by a PSAP to validate locations not received through incoming call signaling.

4.4 MSAG Conversion Service (MCS)

The MSAG Conversion Service provides a convenient way to provide data to, or get data from, a non-upgraded system that still uses MSAG data. This web service provides conversion between PIDF-LO and MSAG data. Two functions are defined:

- PIDFLOtoMSAG: which takes a PIDF-LO, as described in RFC 4119 [6] and updated by RFC 5139 [53] and RFC 5491 [52], and returns an MSAG address as an XML object conforming to NENA 02-010 Version 4, XML Format for Data Exchange;
- MSAGtoPIDFLO: which takes an MSAG address as an XML object conforming to NENA 02-010 Version 4, XML Format for Data Exchange, and returns a PIDF-LO, as described in RFC 4119 and updated by RFC 5139 and RFC 5491.

© Copyright 2011-2022 National Emergency Number Association, Inc.

MSAG Conversion Service is provisioned using the same mechanism as is used to provision the ECRF and LVF: layer replication from the master SI. The layers include all of the layers to create a PIDF-LO as described above, plus a table containing the MSAG field content used prior to NG9-1-1 migration. Field use in MSAGs varies wildly. Nearly every MSAG has some variations from the original NENA data standards as to how fields are used. Because of this variation, the MCS needs a complete set of fields [as defined by NENA-STA-015.10-2018 (originally NENA 02-010v9)] for each MSAG record and a link between the MSAG record and street/address point records in the ECRF/LVF.

Some MSAGs have content in address numbers, and address number suffixes that would not match that in the ECRF/LVF site/structure layer. Address numbers normally use the PIDF-LO fields for the equivalent MSAG fields. When the content differs, an exception record is provided in an MSAG Street Number Exception layer, and a link to that record is included in site/structure.

The PIDFLOtoMSAG function locates the point in the database represented by the input PIDF-LO and retrieves the MSAG data associated with that point. It constructs an MSAG address using any MSAG data available, and the PIDF-LO layers in which MSAG and PIDF-LO are the same. The functions return NENA Version 4 XML data exchange, but the client can convert to any other MSAG version from the XML representation.

The OpenAPI definition of this web service may be found in Appendix E.4.

4.4.1 PIDF-LO to MSAG Conversion

Converts PIDF-LO to MSAG data.

HTTP method: POST

Resource name .../PidfloToMsag

The body of the request MUST contain a PIDF-LO as a string.

A successful query returns an AQS MSAG address as an XML object in a string

Status Codes

200	OK
307	Temporary Redirect
454	Unspecified Error
468	No Address Found
469	Unknown MCS/GCS

© Copyright 2011-2022 National Emergency Number Association, Inc.

4.4.2 MSAG to PIDF-LO Conversion

The MSAGtoPIDFLO function works in the same manner, locating the point in the database to which the MSAG address refers, and composing a PIDF-LO from the PIDF-LO layers.

Converts PIDF-LO to MSAG data.

HTTP method: POST

Resource name .../MsagToPidfLo

The body of the request MUST contain a MSAG address XML component as a string.

A successful query returns a pidfloAddress as a string containing the PIDF-LO

Status Codes

200	OK
307	Temporary Redirect
454	Unspecified Error
468	No Address Found
469	Unknown MCS/GCS

The service logs the invocation of the function, as well as the input and output objects.

Each FE in the MCS MUST implement the server-side of the ElementState event notification package. The MCS MUST promptly report changes in its state to its subscribed elements.

The set of MCS FEs within an ESInet MUST implement the server-side of the ServiceState event notification package for the MCS. It is RECOMMENDED that if there are multiple levels of ESInet within a state, that the state level MCS implement ServiceState as a single service, rather than having a ServiceState for each level of NGCS within the state. In such a service, if any regional or local NGCS' MCS is not operating properly, the state MCS would show some form of non-normal state for the MCS ServiceState.

We observe that the Centerline layer, together with the StreetSegment table and the MCS, can be used to create or re-create an MSAG. For each entry in the centerline layer, construct an MCS PIDFLOToMSAG record with any of the address numbers in the corresponding StreetSegment record. With the remaining information in the centerline and corresponding StreetSegment records, an MSAG record can be created and the set of those records would be a complete MSAG for every address in the database. Some MSAGs contain unusual records for extenuating circumstances that don't have corresponding records in the centerline layer. These would need to be maintained manually.

© Copyright 2011-2022 National Emergency Number Association, Inc.

4.5 Geocode Service (GCS)

The Geocode Service provides geocoding and reverse-geocoding. This web service provides two functions:

- Geocode: which takes a PIDF-LO, as described in RFC 4119 [6], and updated by RFC 5139 [53] and RFC 5491 [52], which contains a civic address, and returns a PIDF-LO containing a geodetic representation for the same location.
- ReverseGeocode: which takes a PIDF-LO as described in RFC 4119 and updated by RFC 5139 and RFC 5491, which contains a geodetic representation, and returns a PIDF-LO that contains a civic address for the same location.

The Geocode Service is provisioned using the same mechanism as is used to provision the ECRF and LVF: layer replication from the master SI. The layers include all of the layers to create a PIDF-LO as described above.

Any conversion, and specifically geocoding and reverse geocoding, can introduce errors. Unless the underlying SI provides very accurate polygons to represent all civic locations precisely, the conversion is complicated by the inherent uncertainty of the measurements and the "nearest" point algorithm employed. Users of these transformation services should be aware of the limitations of the geocoding and reverse geocoding mechanisms. Reverse geocoding is typically less accurate than geocoding, although some error and unquantified uncertainty is inherent in both.

The Geocode function locates a civic address, represented by the input PIDF-LO, by finding a match in its site/structure address points or road centerlines, and uses the matching feature to obtain a geodetic location that represents the civic address. It constructs a PIDF-LO with the geodetic location. If the PIDF-LO in the request contains more than one location, the return must contain only one result, which is the conversion of the first location in the PIDF-LO.

The OpenAPI definition of this web service may be found in Appendix E.5.

4.5.1 GeocodeRequest

Converts civic address to geodetic representation of the location in PIDF-LO format.

HTTP method: POST

Resource name .../Geocode

The body of the request MUST contain a PIDF-LO as a string.

A successful query returns:

© Copyright 2011-2022 National Emergency Number Association, Inc.

GeodecticData

Name	Condition	Description
pidfLoGeo	Conditional, MUST be present if conversion succeeds	PIDF-LO resulting from conversion
gcsReferralUri	Conditional, MUST be present if conversion does not succeed	URI of another GCS

Status Codes

200	Data successfully converted
307	Temporary Redirect
454	Unspecified Error
468	No Address Found
469	Unknown MCS/GCS

4.5.2 ReverseGeocodeRequest

The ReverseGeocode function works in the same manner. It converts geodetic representation of the location to civic address in PIDF-LO format.

HTTP method: POST

Resource name .../ReverseGeocode

The body of the request MUST contain a PIDF-LO as a string.

A successful query returns:

CivicAddress

Name	Condition	Description
PIDFLOAddress	Conditional, MUST be present if conversion succeeds	PIDF-LO resulting from conversion
gcsReferralUri	Conditional, MUST be present if conversion does not succeed	URI of another GCS

Status Codes

© Copyright 2011-2022 National Emergency Number Association, Inc.

200	Data successfully converted
307	Temporary Redirect
468	No Address Found
469	Unknown MCS/GCS

The service logs the invocation of the function, as well as the input and output objects. Each FE in the GCS must implement the server-side of the ElementState event notification package. The GCS must promptly report changes in its state to its subscribed elements.

The set of GCS FEs within an ESInet MUST implement the server-side of the ServiceState event notification package for the GCS. It is RECOMMENDED that if there are multiple levels of ESInet within a state, that the state level GCS implement ServiceState as a single service, rather than having a ServiceState for each level of NGCS within the state. In such a service, if any regional or local NGCS' GCS is not operating properly, the state GCS would show some form of non-normal state for the GCS ServiceState.

4.6 PSAP

A PSAP is a service, typically composed of more than one functional element. The functional elements that make up a PSAP are defined in NENA STA-023.1-202Y, *NG9-1-1 PSAP Specifications for the NENA i3 Solution* (forthcoming). A PSAP provides the following interfaces towards the ESInet.

4.6.1 SIP Call interface

The PSAP MUST deploy the SIP call interface as defined in Section 3.1 including the multimedia capability, and the non-interactive call (emergency event) capability. PSAPs MUST recognize calls to their administrative numbers received from the ESInet (and distinguishable from normal 9-1-1 calls by the presence of the number in a sip or tel URI in the To header field and the absence of the sos service URN in a Request-URI line, and identified in the target PSAP's SALR, if available). The SIP call interface MAY also be used to place non 9-1-1 calls (including callbacks) from the PSAP. Such outbound calls will be routed to the OCIF of the serving ESInet/NGCS for processing and routing. Callback and other non-emergency outbound call INVITE messages MUST comply with the SIP call interface as defined in Section 3.1, and constructed using the guidance provided in section 4.20 (OCIF), with the following clarifications. The To header field value of the callback INVITE message MUST be set to a value that will allow reaching the home network of the target. If the To header field value is a tel URI, the OCIF will route the callback toward the PSTN, which means that only the voice portion will go through. If the To header field value is a sip URI, the domain SHALL be the one of the home network of the target. The Request-URI line SHOULD contain the same URI value as in the To header field.

© Copyright 2011-2022 National Emergency Number Association, Inc.

The PSAP can use a number of techniques to determine the best route for the call to the home network of the target. Specifically for emergency callbacks, the PSAP MAY rely on the domain available in the P-A-I (preferred) or From header field of the original emergency call from a fixed wireline-type network. For mobile networks supporting roaming and other IMS-based networks, the PSAP MAY rely on the domain found in the "orig-ioi" parameter of a P-Charging-Vector (RFC 7315 [209]) header field or alternatively, in a P-Charge-Info header field (RFC 8496 [208]) of the original emergency call, if available. The domain of the home network is to be populated in the Request-URI line and the To header field of the callback INVITE message.

Outbound calls MAY be placed via the ESInet using the ESRP as an outgoing proxy server (see Section 4.2.2.1). In most circumstances the ESRP will forward calls to the OCIF, which uses a Network-to-Network Interface to an interconnected network as described in section 4.20.

Note: Handling of media other than voice-only callbacks is incompletely specified and will be addressed in a future version of this document.

4.6.2 Media

All i3 PSAPs MUST support all media, voice, video, and text. If a PSAP receives an Offer containing both MSRP and RTT, it SHOULD send an Answer with only one of them. If the PSAP receives an Answer containing both RTT and MSRP, it MUST be prepared to deal with both simultaneously. When placing callbacks, PSAPs SHOULD offer all supported media choices, subject to operational considerations.

Emergency calls marked with a humintlang tag (RFC 8373) [173] SHOULD be processed with appropriate language-specific resources available to the PSAP. SDP offers and answers generated by the PSAP MUST include appropriate language tags. Answers to offers that included language tags MUST include language tags. The PSAP is not obligated to offer languages it supports with outside entities such as a language translation service.

Note that a future edition of this document will include a standard method to invoke a language translation service using the humintlang (RFC 8373) [173] mechanism.

4.6.3 LoST interface

The PSAP MUST implement a LoST client interface as defined in Section 3.4. The PSAP uses the ECRF and LVF to handle calls that must be dispatched and calls that must be transferred based on the actual location of the incident. The LoST interface is used with the "urn:emergency:service:responder" URNs to achieve "selective transfer" operations. The PSAP would query the ECRF using LoST with the appropriate responder URN and the location of the incident. It would receive the URI to which the call should be directed.

© Copyright 2011-2022 National Emergency Number Association, Inc.

The PSAP MAY also use the LoST interface to find an AgencyLocator URI by location by querying the ECRF with a service URN of a subservice of "urn:emergency:service:serviceagencylocator". The AgencyLocator record can be retrieved from the URI by dereferencing it with HTTPS GET. [4.15.1] The Agency Locator record document is returned. From the AgencyLocator record, other interface points, such as a URI to which to send an EIDO, may be found.

4.6.4 LIS Interfaces

The PSAP MUST implement both SIP Presence Event Package and HELD dereferencing interfaces to any LIS function as described in Section 4.10. When the PSAP receives a location reference (in a Geolocation header field on the upstream SIP interface[38]) it uses the LIS dereferencing interface to obtain a location value. The PSAP MUST be able to be provisioned with credentials for every LIS in its service area[39]. The PSAP MUST use TCP with TLS for the LIS dereferencing interface, with fallback to TCP (without TLS) on failure to establish a TLS connection when TLS is used. The PSAP SHOULD maintain persistent TCP (and TLS when used) connections to LISes with which it has frequent transactions. A suggested value for "frequent" is more than one transaction per day.

For HELD location URIs, specifying responseTime = emergencyDispatch should result in a location meeting current regulatory accuracy requirements. If the PSAP wishes an immediate location, it can specify a short responseTime (perhaps 250 ms), and get the best location quality available in that amount of time. Location updates for location URIs using HELD may be obtained by repeating the dereference request.

PSAPs receiving SIP location URIs SHOULD subscribe to the Presence event per RFC 3856 [25] in order to receive the location value. In response to a subscribe request, the PSAP receives an immediate location report, which may reflect the best available location at the time of the subscription. A subsequent location update is sent when more accurate location information is available. By setting the expiration time of the subscription, the PSAP is able to control which updates it receives. PSAPs that wish to track the motion of a caller could use the location filter and event rate control mechanisms (RFC 6447) [72] and rate-control (RFC 6446) [80] to control updates.

---

[38] If the PSAP receives a call via a transfer from another agency, the location of the caller will be found in the EIDO included in the transfer and not in a Geolocation header.

[39] This document specifies that the LIS accept credentials issued to the PSAP traceable to the PCA. Notwithstanding that requirement, ESInet elements needing location, including PSAPs, must be able to be provisioned with credentials acceptable to LISes that do not accept the PCA credential.

© Copyright 2011-2022 National Emergency Number Association, Inc.

Note that because the PSAP will not have an identity of an arbitrary device with which it could query a LIS to get the device's location, the "manual ALI query" function, also known as "Reverse-ALI" in E9-1-1, has no equivalence in NG9-1-1.

4.6.5 Bridge Interface

A PSAP MAY deploy a bridge (as described in Section 4.7) inside the PSAP, in which case it MUST provide the bridge controller interfaces. PSAPs MUST be able to accept calls from, and utilize the features of, outside bridges.

4.6.6 ElementState

The PSAP MUST deploy an ElementState Notifier. Any element inside a PSAP that provides a call queue MUST deploy an ElementState notifier as described in Section 2.4.1.

4.6.7 ServiceState

The PSAP MUST deploy a ServiceState notifier as described in Section 2.4.2.

4.6.8 AbandonedCall Event

The PSAP MUST implement the subscriber side of the AbandonedCall Event as described in Section 4.2.2.9.

4.6.9 DequeueRegistration

The PSAP MUST implement a DequeueRegistration client, as described in Section 4.2.1.4, for every queue on which it expects to receive calls. When the PSAP registers, it specifies a URI to direct calls to it. That URI will appear in the top Route header field when the PSAP receives an emergency call or the Request-URI on an admin call. If that URI is constructed appropriately, the PSAP can identify which queue inside the PSAP to which the call is destined.

4.6.10 QueueState

The PSAP MUST implement a QueueState notifier as described in Section 4.2.1.3 for all queues it manages.

© Copyright 2011-2022 National Emergency Number Association, Inc.

4.6.11 SI

The PSAP MAY provide[40] a GIS server interface, as described in Section 3.6, for the ECRF, GIS Replica, and other interfaces. The PSAP MAY provide the MSAG Conversion Service (server side) or MAY use an ESInet service (client side).

4.6.12 Logging Service

The PSAP MUST implement a Logging Service client, as defined in Section 4.12, including the client side of the media recording mechanism (Section 4.12.2). Provisioning controls whether the PSAP records media. The PSAP MAY deploy a Logging Service (as described in Section 4.12) inside the PSAP, in which case it MUST provide the Logging Service retrieval functions. A PSAP MUST be able to use a Logging Service hosted in the ESInet.

4.6.13 Security Posture

The PSAP MUST provide a Security Posture notifier as described in Section 2.4.2.

4.6.14 Policy

The PSAP MAY provide a Policy Store as described in Section 3.3.1, in which case it MUST implement the server-side of the policy retrieval functions, and MAY provide the server-side of the policy storage function. The PSAP MAY provide a Policy Editor, in which case it MUST deploy the client-side of the policy retrieval and storage functions. If the PSAP uses a Policy Store outside the PSAP to control functions inside the PSAP, it MUST deploy the client-side of the policy retrieval functions.

PSAPs MUST provide a RoutePolicy in the upstream PRF for the queue(s) to which its calls are sent. PSAPs MUST also provide an Enqueuer policy to specify which entities are allowed to send it calls.

4.6.15 Additional Data Dereference

The PSAP MUST deploy a dereference (HTTPS GET) interface for additional data as described in Section 7, as well as the IS-ADR identity query mechanism. Local PSAP policy MAY dictate which Additional Data, if any, is retrieved and used. The PSAP MUST also be able to dereference an EIDO URI for a call transferred to it.

[40] The GIS system may be provided by a 9-1-1 Authority.

© Copyright 2011-2022 National Emergency Number Association, Inc.

4.6.16 Time Interface

The PSAP MUST implement an NTP client interface for time of day information. The PSAP MAY also provide an interface to a hardware clock.

4.6.17 Test Call

PSAPs MUST support the test call interface as described in Section 9, although administrative provisioning processes SHOULD be available to disable it, especially under overload conditions. The test interface includes the ability of the test caller to offer media, receive a response, and loop back a small number of packets of each media accepted at the PSAP. PSAPs MUST support test of all media – voice, video, and text.

PSAPs may wish to arrange to have test calls sent to it periodically from a known source so that it can be assured that calls from outside the ESInet can get to the PSAP. For that purpose, a "Test Call Generator" Functional Element may be used that the PSAP can control. The Test Call Generator interface includes a Web Service with a single function: SendCallRequests. The OpenAPI definition of this web service may be found in Appendix E.6.

4.6.17.1 SendCallRequests

Updates an existing send call request identified by the PSAP ID or creates a new one if the request does not exist.

HTTP method: PUT

Resource name .../ SendCallRequests/{psapId}:

Parameters:

Name	Condition	Description
psapId	MANDATORY	AgencyId of the PSAP that wishes to have test calls sent to it
location	MANDATORY	PIDF-LO used for location of test calls
frequency	MANDATORY	Minutes between test call send
discrepancyRateLimit	MANDATORY	Max number of Discrepancy Reports per hour
startDate	MANDATORY	When to start sending test calls
endDate	MANDATORY	When to stop sending test calls

© Copyright 2011-2022 National Emergency Number Association, Inc.

Name	Condition	Description
testConditions	OPTIONAL	PrrTest conditions (see below) for the test

Status Codes

200 OK
442 Unacceptable Parameters
454 Unspecified Error
458 Policy Violation

4.6.18 Testing of Policy Rules

To be able to test that the ruleset for a particular nominal next hop works as expected, the test call MAY include a Call-Info header field with a purpose parameter of "emergency-prr-test". The data retrieved from the URI in the Call-Info header field is a JSON data structure that contains a list of name/value pairs. The names are strings that would be legal as a single component in the condition portion of a PRR rule (not allowing AND/OR). The structure includes the hostname of an ESRP and the unique ID (FQDN) of a "nominal next hop". The ESRP processing such a test call, if it is named in the structure, and the nominal next hop is named in the structure, sets the elements in the list to the corresponding values, rather than the actual values, when it evaluates the ruleset.

PrrTest

Name	Condition	Description
hostName	MANDATORY	ESRP Hostname that test conditions are specified for
nominalNextHop	MANDATORY	URI of for nominal next hop that rule set conditions are applied to
conditions	MANDATORY (may be repeated)	Array

The conditions array contains:

© Copyright 2011-2022 National Emergency Number Association, Inc.

Name	Condition	Description
name	MANDATORY	One of TimePeriodCondition, SipHeaderCondition, AdditionalDataCondition, MimeBodyCondition, LocationCondition, CallSuspicionCondition, QueueStateCondition, LostServiceUrnCondition, ServiceStateCondition, CallSourceCondition, BodyPartCondition, RequestUriCondition, NormalNextHopCondition, IncomingQueueCondition, SdpOfferCondition, CapCondition, CallingNumberVerificationStatusCondition]
value	MANDATORY	Value of the condition (as a string)

These test calls MUST originate from within the ESInet and MUST come from an entity with credentials traceable to the PCA and trusted by the ESRP. The ESRP has a policy (TestCalls) that specifies which originators (the identifier in the credential) from which it will process PRR test calls. The URIs are dereferenced with an HTTPS GET protected by TLS. The credentials used by the server MUST be traceable to the PCA and MUST occur in the ESRP policy.

More than one Call-Info URI with a purpose of "emergency-prr-test" may occur in a test call, each with unique combinations of ESRP and nominal-next-hop targets.

4.6.19 Call Diversion

A PSAP may become overloaded and be unable to answer every call. Overload is determined by exceeding the size of the primary queue to which its calls are sent. Routing rules for the PSAP would then cause calls to receive an alternate call treatment:

- Calls can be sent a "Busy" indication;
- Calls can be diverted to an Interactive Media Response unit;
- Calls can be diverted to one or more alternate PSAPs.

The latter is mechanized by sending the call to queues that other PSAPs dequeue. Since the diverted-to PSAP(s) must explicitly permit (via the Enqueuer policy and possibly DequeueRegistration) calls to be placed on its queues, no calls can be sent to a PSAP that hasn't explicitly asked for them.

© Copyright 2011-2022 National Emergency Number Association, Inc.

PSAPs that agree to take calls from other PSAPs may require explicit management approval at the time the calls are sent. Effectively, such PSAPs are agreeing to take calls on a standby basis only, and explicit management action is required before the calls will actually be accepted.

To accomplish this, the diverted-to PSAP registers to the DequeueRegistration of the diverted-from PSAP. The diverted-from PSAP subscribes to the QueueState event for the diversion queue, but the diverted-to PSAP will have the "Standby" parameter set to "true". It may specify a filter that limits notifications to those setting QueueState to "DiversionRequested". When the QueueState event notification occurs with "DiversionRequested" state, the diverted-to PSAP management would be alerted. If it agrees to accept calls, it would change its QueueState Standby parameter to "false", and calls would subsequently be sent to it. When the diverted-to PSAP determines that its services are no longer needed, it can reinstate the Standby to "true".

4.6.20 Incidents

A new emergency call arrives with a new Incident Tracking Identifier already assigned. Initially, each emergency call is a new Incident. The call taker may determine that the call is actually part of another Incident, usually reported in a prior call. The PSAP MUST merge the IncidentTrackingID assigned by the ESRP with the actual IncidentTrackingID. It does so with the IncidentMergeEvent log record and sends an EIDO with a Merge Information component. Incidents can also be linked or split as described in the Logging Service (Section 4.12). The actual IncidentTrackingID would be part of the EIDO object passed to a secondary PSAP or responder and part of the INVITE if the call is transferred. When the PSAP completes processing of an Incident, it logs a IncidentClearEvent record.

4.7 Bridging and Transfers

Bridging is used in NG9-1-1 to transfer calls and conduct conferences. Bridges have a SIP signaling interface to create and maintain conferences and media mixing capability. Bridges MUST be multimedia capable (voice, video, text). A bridge is necessary to transfer a call because IP-based devices normally cannot mix media, and transferring always adds the new party (for example, a call taker at a transfer-to PSAP) to the call before the transferor (for example, the original call taker at the PSAP which initially answered the call) drops off the call.

4.7.1 Attended Transfers

This document describes two ways that bridging is employed. One way is termed "ad hoc" and is characterized by using a bridge only when it is needed during transferring or conferencing more than two parties.

© Copyright 2011-2022 National Emergency Number Association, Inc.

The rough transfer sequence for ad hoc, based on the procedures defined in RFC 4579[41] [39], is:

1. PSAP creates a conference on the bridge
2. PSAP REFERs the caller to the bridge
3. PSAP tears down the original PSAP-Caller leg
4. PSAP REFERs transfer target (transfer-to PSAP for example) to the conference
5. PSAP tears down its leg to the conference, the transfer-to PSAP and the caller remain
6. Transfer-to PSAP REFERs the caller to it
7. Transfer-to PSAP terminates the conference.

Note: When the caller drops voluntarily or involuntarily from the ad hoc Bridge, leaving only two participants, the ad hoc bridge must identify which participant will release the bridge resources. This can be achieved by moving the host in the <host-info> element on the conference subscription's NOTIFY. A future revision of this document will normatively specify this behavior.

Some calling devices may not support the Replaces header field (which can be determined by examining the content of the Supported header field to see if a "replaces" option tag is present, or by completing an OPTIONS transaction and obtaining the Accept header field that way). If the calling device does not support the Replaces header field, then a B2BUA in the path MUST be present which does support the Replaces header field in an ESInet supporting ad hoc bridging. Often, this B2BUA will be part of the BCF. All calls are relayed through the B2BUA. The B2BUA is transparent to signaling with the following exceptions:

1. The Contact URL is modified to be a URL of the B2BUA for both the caller (Contact in INVITE) and PSAP (Contact in 200 OK).
2. The REFER method, when executed on the PSAP side to a conference bridge, causes the bridge to invite the B2BUA to the conference, and the B2BUA to respond as illustrated below. The leg between the caller and the B2BUA sees no transaction.
3. If the B2BUA receives an INVITE from a caller that does not include a Supported header field containing the "replaces" option-tag, it MUST include a Supported

[41] The ad hoc method described in this document functionally adheres to RFC 4579 however the terminology used herein may differ. For example, the "Bridge" relates to the "Focus" application in RFC 4579 and the "Conference Application" relates to the "Conference-Factory" application in RFC 4579. The terms used herein should be interpreted broadly to support functionalities defined in RFC 4579.

© Copyright 2011-2022 National Emergency Number Association, Inc.

header field containing the "replaces" option-tag in the INVITE forwarded to the ESInet and provide the functionality described in this section.

4. Media endpoints towards both the caller and the PSAP MAY be rewritten to be contained within the B2BUA.

The other mechanism is "Route All Calls Via a Conference Aware UA". In this mechanism, at least the signaling portion of a bridge is always in the call path, and transfer is accomplished by adding and deleting parties to the bridge. An element in the call path effectively operates as a B2BUA, modifying the call signaling towards the PSAP and the response to the caller so that it appears as a bridge in the path, and, when transfer is actually needed, what was a B2BUA operates as a true bridge, allowing the transfer-to PSAP to be added to the bridge and the transfer-from PSAP to drop from the bridge. Often, a media mixer is not in the path unless needed.

The high-level transfer sequence for this method is:

1. The original call arrives at a conference-aware UA.
2. The conference-aware UA acts as a B2BUA and modifies the signaling towards the PSAP by adding the conference marker ("isfocus") and modifying the Contact to be itself rather than the caller.
3. The PSAP gets the call, and responds in the normal way. The response to the initial call will be sent to the conference-aware UA.
4. The conference-aware UA modifies the response from the PSAP towards the caller by adding the conference indicator, and modifies the Contact to identify itself. It MAY NOT modify the SDP, so the media is set up directly between the caller and the PSAP.
5. At some point, the PSAP desires to transfer the call to a transfer-to PSAP. Since it has the 'isfocus' from the conference UA already, it sends the conference-aware UA a REFER to ask it to add the transfer-to PSAP to the conference.
6. The conference-aware UA sends an INVITE to the transfer-to PSAP. It also MAY re-INVITE both the caller and the transfer-from PSAP, including SDP that moves the media to a media mixer if it was not already connected to one. The conference-aware UA is now acting as a normal bridge.
7. All parties accept their INVITEs and a 3-way conference with media mixing ensues.
8. The transfer-from PSAP then leaves the conference by sending a BYE.
9. The conference-aware UA then MAY re-INVITE the caller and the transfer-to PSAP, including signaling that will move the media to be direct between the transfer-to PSAP and the caller.

All Bridges in the ESInet/NGCS MUST implement the Session Recording Client interface defined by SIPREC (RFC 7866) [116]. Provisioning MAY control whether the bridge does log media.

© Copyright 2011-2022 National Emergency Number Association, Inc.

When the bridge is used to transfer the call, the location of the caller and any Additional Data included (or retrieved in conjunction) with the call MUST be transferred to the transfer target. The NENA Call Identifier and the NENA Incident Tracking Identifier MUST be copied from the REFER to the outgoing INVITE. The REFER MUST contain a suitable URN, usually the urn used to query the ECRF to determine the correct responder, or an appropriate urn from the urn:emergency:service:responder tree if a specific responder was selected, a 'serviceurn' parameter of the Refer-To . A misrouted call being transferred to the proper PSAP would typically be urn:service:sos, but could be urn:emergency:service:psap if the ECRF was not used to reroute the call. The Refer-To header field contains the URI of the target (which may be returned from a LoST query) and MUST contain the URN (in the urn:service:sos or urn:emergency:service:sos trees) as a URI parameter of 'serviceurn'. The REFER to the bridge has the bridge's URI in the To: and in the Request-URI. It also contains a Referred-By header field (RFC 3892) [28] with the URI of the primary PSAP. When the INVITE is created by the bridge to the secondary PSAP, the INVITE MUST contain the service URN in the Request-URI, with a Route header field containing the URI (which should include the "lr" parameter to avoid Request-URI rewriting) found in the Refer-To header field, and MUST contain a Referred-By header field with the URI of the primary PSAP per RFC 3892. S/MIME protection of the referrer is OPTIONAL. If there was no 'serviceurn' parameter and there is an EIDO, the bridge sets the Request-URI to urn:emergency:service:sos. Additionally, any information the PSAP has determined beyond what it was sent SHOULD be given to the transfer target. The mechanism for accomplishing this is to create an EIDO and include it "by reference" in the transfer operation. The transferor creates the EIDO and includes a reference to the EIDO in a Call-Info header field with a purpose parameter of "emergency-eido" as an escaped header field in the Refer-To header field. Note that the Refer-To header field MUST be a sip URI. Tel URIs do not support purpose parameters. The bridge will then include this header field in the INVITE it sends to the transfer target. The EIDO includes the location reported for the caller (in the form it received it, i.e., by-value or by-reference), the callback number, and any Additional Data included (or retrieved in conjunction with) the call. (See Section 4.7.2 for further discussion.) An example of the associated header fields is shown below.

```
REFER sip:+12125551234@OSP-Provider.com SIP/2.0
…
Refer-To:<sip:Poison-Control@cnty.st.us?Call-
Info=%3Chttps%3A%2F%2FNG911PSAP-A.911Authority-
A.net%2Feido09245673%3E%3Bpurpose%3Demergency-eido>

…
```

The bridge is a service: each element of the bridge MUST implement the server-side of ElementState and the set of bridge elements MUST implement the server-side of

© Copyright 2011-2022 National Emergency Number Association, Inc.

ServiceState. As bridges are typically a local service, it is RECOMMENDED that ServiceState for the bridge service be implemented by each NGCS that provides a bridge service. For the Ad Hoc case, the transfer-to PSAP MUST release the bridge when the transfer-from PSAP terminates its leg of the call in order to release bridge resources.

As discussed in Section 5.7 of NENA 08-002 [70], there is a problem in that some devices which could originate 9-1-1 calls do not support the Replaces header field. If a PSAP needs to transfer a call originated by such a device, it cannot use the standardized SIP signaling to the caller as described above. With Route All Calls Via a Conference-Aware UA, the conference-aware UA never changes the leg towards the caller (unless it must re-INVITE to change SDP if the initial media was negotiated directly between the caller and the PSAP). Thus, the calling device need not support the Replaces header field. For the ad hoc method, to support devices that do not implement the Replaces header field, a Back-to-Back User Agent is needed between the caller and the bridge/PSAP. Often the B2BUA will be located in the BCF, because most commercial Session Border Controllers which are deployed within a BCF have that functionality built in. Some SBCs may "anchor" media, meaning that they terminate the caller's media at the B2BUA and relay it towards the PSAP or bridge. Others may only affect the signaling. The B2BUA element will always be in the path for all callers if deployed, especially if it is part of the BCF but may not affect the signaling for callers that indicate support for Replaces.

Conferencing procedures are documented in RFC 4579 [39]. This document includes definition of an Event package that allows conference participants to manage the conference. In the message sequences below, all participants are conference-aware (that is, they implement the event package). It is not necessary for the caller to be conference-aware. If the caller is not conference aware, the SUBSCRIBE to the conference package does not occur. The caller, or some element in the path, MUST implement the Replaces header field (see Section 3.1.1.2). Three scenarios are illustrated below: Ad Hoc without B2BUA, Ad Hoc with B2BUA- and Route All Calls Via a Conference-Aware UA.

4.7.1.1 SIP Ad Hoc Flow with No B2BUA on Ingress Call Path

4.7.1.1.1 Creation of a Conference

This scenario described in the call flow depicted below follows Section 5.4 of RFC 4579 [39].

© Copyright 2011-2022 National Emergency Number Association, Inc.

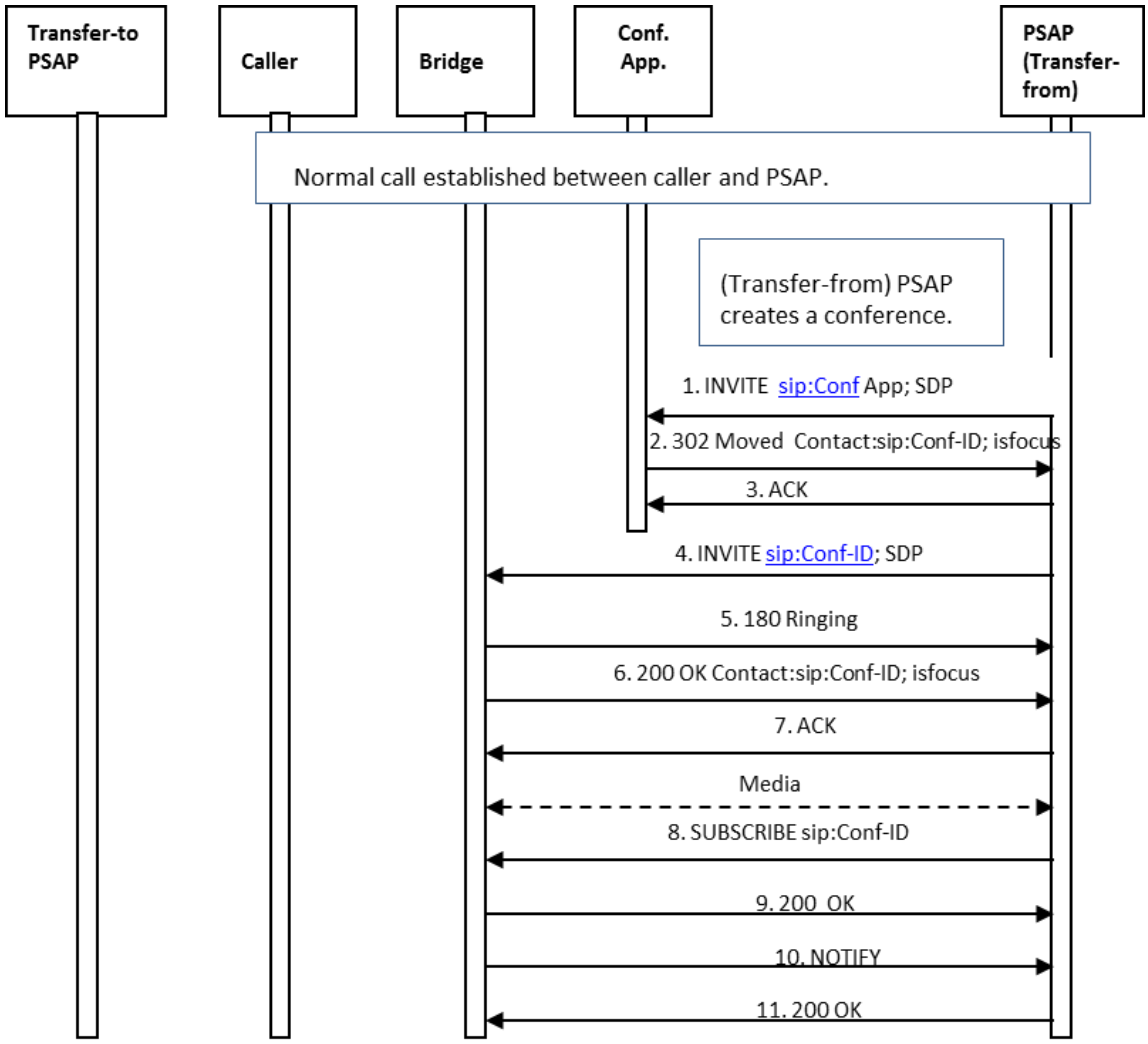


Figure 4-1. Ad Hoc Conference Call Flow Using SIP

1. The transfer-from PSAP creates a conference by first sending an INVITE with specified Media in the SDP to a conference application, using a URI that is known by/provisioned at the transfer-from PSAP.
2. The Conference Application responds by sending a 302 Moved message, which redirects the transfer-from PSAP to the conference bridge and provides the Conference URI that SHOULD be used for the conference.
3. The transfer-from PSAP acknowledges the receipt of the 302 Moved message.

© Copyright 2011-2022 National Emergency Number Association, Inc.

4. The transfer-from PSAP generates an INVITE with specified Media in the SDP to establish a session with the conference bridge[42].
5. The conference bridge responds to the INVITE by returning a 180 Ringing message.
6. The conference bridge then returns a 200 OK message, and a media session is established between the transfer-from PSAP and the conference bridge.
7. The transfer-from PSAP returns an ACK message in response to the 200 OK.

Media: If SDP includes media-type specification for audio and/or video and/or RTT, then RTP media is exchanged. If SDP includes media-type specification for MSRP, then MSRP messages are exchanged.

8. through 11. Once the media session is established, the transfer-from PSAP subscribes to the conference associated with the URI obtained from the Contact header field provided in the 200 OK message from the conference bridge.

4.7.1.1.2 Transfer-from PSAP Asks Bridge to Invite the Caller to the Conference

This flow is based on Section 5.10 of RFC 4579 [39].

[42] Note that, based on RFC 4579, the messages sent in Steps 2, 3, and 4 are optional and may not be exchanged if the conference application and the media server are the same.

© Copyright 2011-2022 National Emergency Number Association, Inc.

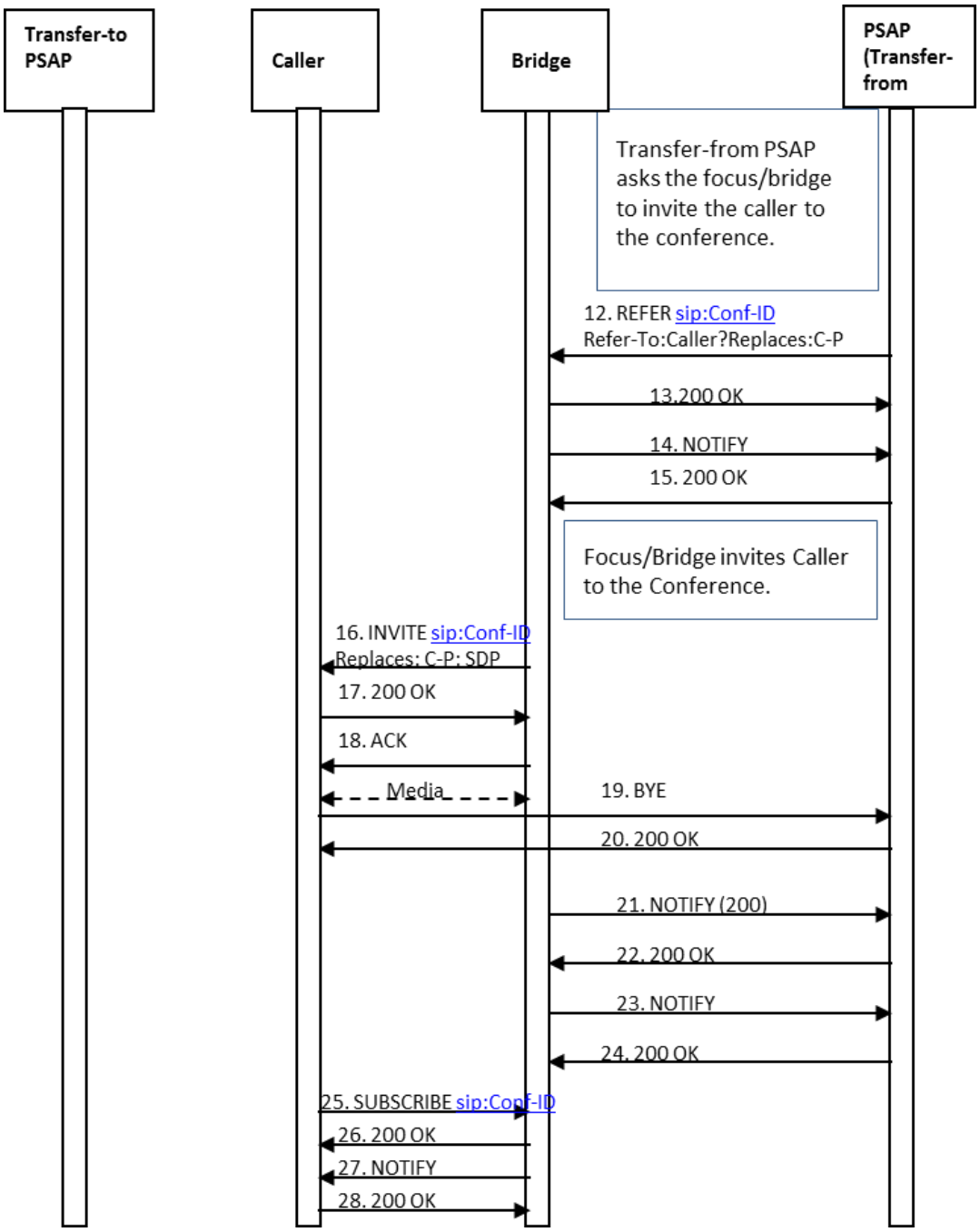


Figure 4-2 Transfer-from PSAP Asks Bridge to Invite the Caller to the Conference

12. After the transfer-from PSAP establishes the conference, it sends a REFER method to the conference bridge asking it to invite the caller to the conference. The REFER

© Copyright 2011-2022 National Emergency Number Association, Inc.

method contains an escaped Replaces header field value in the URI included in the Refer-To header field.

13. The bridge returns a 200 OK message to the transfer-from PSAP.
14. The bridge then returns a NOTIFY message, indicating the subscription state of the REFER request (i.e., active).
15. The transfer-from PSAP returns a 200 OK in response to the NOTIFY message.
16. The bridge invites the caller to the conference by sending an INVITE method containing the Conference URI and a Replaces header field that references the leg between the caller and the transfer-from PSAP and specified Media in the SDP.
17. The caller accepts the invitation by returning a 200 OK message.
18. The bridge acknowledges receipt of the 200 OK message by returning an ACK.

A media session is established between the caller and the bridge.

If SDP includes media-type specification for audio and/or video and/or RTT, then RTP media is exchanged. If SDP includes media-type specification for MSRP, then MSRP messages are exchanged.

19. The caller releases the connection to the transfer-from PSAP by sending a BYE message.
20. The transfer-from PSAP responds by returning a 200 OK message.
21. The bridge sends a NOTIFY message to the transfer-from PSAP to provide REFER processing status.
22. The transfer-from PSAP responds by returning a 200 OK message.
23. The bridge sends a NOTIFY message to the transfer-from PSAP to provide updated status associated with the conference state.
24. The transfer-from PSAP responds by returning a 200 OK message.
25. The caller subscribes to the conference associated with the Conference URI provided in the INVITE message from the bridge by sending a SUBSCRIBE message to the bridge. (Optional)
26. The bridge acknowledges the subscription request by sending a 200 OK message back to the caller. (Optional)
27. The bridge then returns a NOTIFY message to the caller to provide subscription status information. (Optional)
28. The caller responds by returning a 200 OK message. (Optional)

4.7.1.1.3 Transfer-to PSAP is Invited to the Conference

This flow is based on Section 5.5 of RFC 4579 [39].

© Copyright 2011-2022 National Emergency Number Association, Inc.

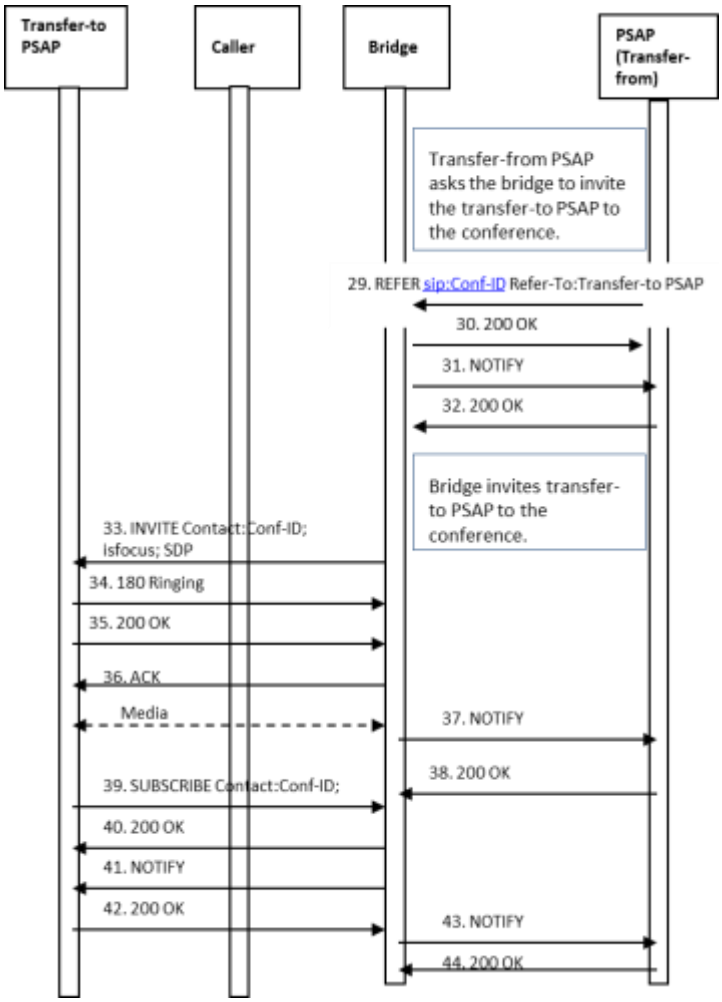


Figure 4-3 Secondary PSAP Invited to Conference

29. The transfer-from PSAP sends a REFER method to the conference bridge asking it to invite the transfer-to PSAP to the conference. The REFER method contains the Conference URI and a Refer-To header field that contains the URI of the transfer-to PSAP. The REFER method also contains an escaped Call-Info header field value containing a reference URI that points to the EIDO data structure and a purpose parameter of ”emergency-eido”.
30. The bridge returns a 200 OK message to the transfer-from PSAP.
31. The bridge then returns a NOTIFY message, indicating that subscription state of the REFER request (i.e., active).
32. The transfer-from PSAP returns a 200 OK in response to the NOTIFY message.
33. The bridge invites the transfer-to PSAP to the conference by sending an INVITE method with SDP containing the Conference URI and Contact header field that

© Copyright 2011-2022 National Emergency Number Association, Inc.

contains the Conference URI and the 'isfocus' feature parameter. The INVITE contains the Call-Info header field containing a reference URI that points to the EIDO data structure and a purpose parameter of "emergency-eido".

34. The transfer-to PSAP UA responds by returning a 180 Ringing message to the bridge.
35. The transfer-to PSAP accepts the invitation by returning a 200 OK message.
36. The bridge acknowledges receipt of the 200 OK message by returning an ACK.

A media session is established between the transfer-to PSAP and the bridge.

If SDP includes media-type specification for audio and/or video and/or RTT, then RTP media is exchanged. If SDP includes media-type specification for MSRP, then MSRP messages are exchanged.

37. The bridge returns a NOTIFY message to the transfer-from PSAP to provide updated status of the subscription associated with the REFER request.
38. The transfer-from PSAP responds to the NOTIFY message by returning a 200 OK message.
39. The transfer-to PSAP subscribes to the conference associated with the Conference URI provided in the INVITE message from the bridge by sending a SUBSCRIBE message to the bridge.
40. The bridge acknowledges the subscription request by sending a 200 OK message back to the transfer-to PSAP.
41. The bridge then returns a NOTIFY message to the transfer-to PSAP to provide subscription status information.
42. The transfer-to PSAP responds by returning a 200 OK message.
43. The bridge sends a NOTIFY message to the transfer-from PSAP providing updated status for the subscription associated with the REFER request.
44. The transfer-from PSAP responds to the NOTIFY message by returning a 200 OK message.

At this point the caller, transfer-from PSAP, and transfer-to PSAP are all participants in the conference.

© Copyright 2011-2022 National Emergency Number Association, Inc.

4.7.1.1.3.1 Transfer-from PSAP Drops Out of Conference; Transfer-to PSAP Completes Transfer

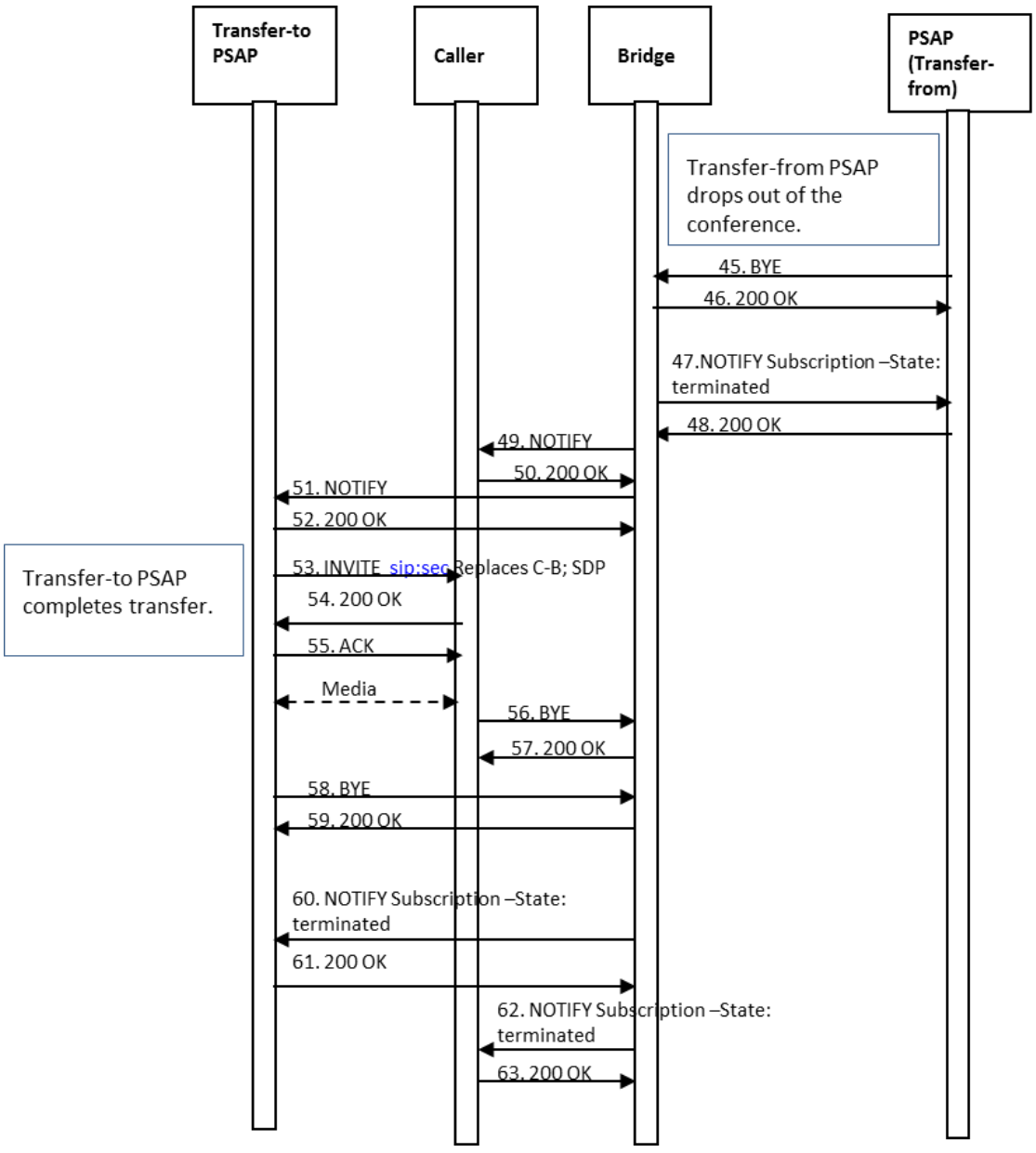


Figure 4-4 Transfer-from PSAP Drops, Transfer-to PSAP Completes Transfer

45. Upon determining that the emergency call transfer should be completed, the transfer-from PSAP disconnects from the call by sending a BYE message to the bridge.

© Copyright 2011-2022 National Emergency Number Association, Inc.

46. The conference bridge responds by returning a 200 OK message.
47. The bridge then returns a NOTIFY message indicating that the subscription to the conference has been terminated.
48. The transfer-from PSAP returns a 200 OK in response to the NOTIFY.
49. The bridge then returns a NOTIFY message to the caller indicating that there has been a change to the subscription state. (Optional)
50. The caller returns a 200 OK in response to the NOTIFY. (Optional)
51. The bridge returns a NOTIFY message to the transfer-to PSAP indicating that there has been a change to the subscription state.
52. The transfer-to PSAP returns a 200 OK in response to the NOTIFY.
53. Upon recognizing that the caller and the transfer-to PSAP are the only remaining participants in the conference, the transfer-to PSAP completes the transfer by sending an INVITE to the caller requesting that they replace their connection to the bridge with a direct connection to the transfer-to PSAP. The transfer-to PSAP learns the URI of the caller through the entity attribute in the endpoint section of the user's container in the conference NOTIFY from the bridge.
54. The caller responds by returning a 200 OK message to the transfer-to PSAP.
55. The transfer-to PSAP returns an ACK in response to the 200 OK.

A media session is established between the transfer-to PSAP and the caller.
If SDP includes media-type specification for audio and/or video and/or RTT, then RTP media is exchanged. If SDP includes media-type specification for MSRP, then MSRP messages are exchanged.

56. The caller then sends a BYE to the bridge to terminate the session.
57. The bridge responds by sending the caller a 200 OK message.
58. The transfer-to PSAP also terminates its session with the bridge by sending a BYE message to the bridge.
59. The bridge responds by sending a 200 OK message to the transfer-to PSAP.
60. The bridge then returns a NOTIFY message to the transfer-to PSAP indicating that the subscription to the conference has been terminated.
61. The transfer-to PSAP returns a 200 OK in response to the NOTIFY message.
62. The bridge sends a NOTIFY message to the caller indicating that the subscription to the conference has been terminated. (Optional)
63. The caller responds with a 200 OK message. (Optional)

At this point, the transfer is complete, and the caller and the transfer-to PSAP are involved in a two-way call.

© Copyright 2011-2022 National Emergency Number Association, Inc.

4.7.1.2 SIP Ad Hoc Method with B2BUA in the Ingress Call Path

This scenario is the same as above with the addition of the B2BUA for calling devices that do not support the Replaces header field. In this example, the B2BUA anchors media, although not all B2BUAs will do that.

4.7.1.2.1 Initial Call and Initial Conference Creation

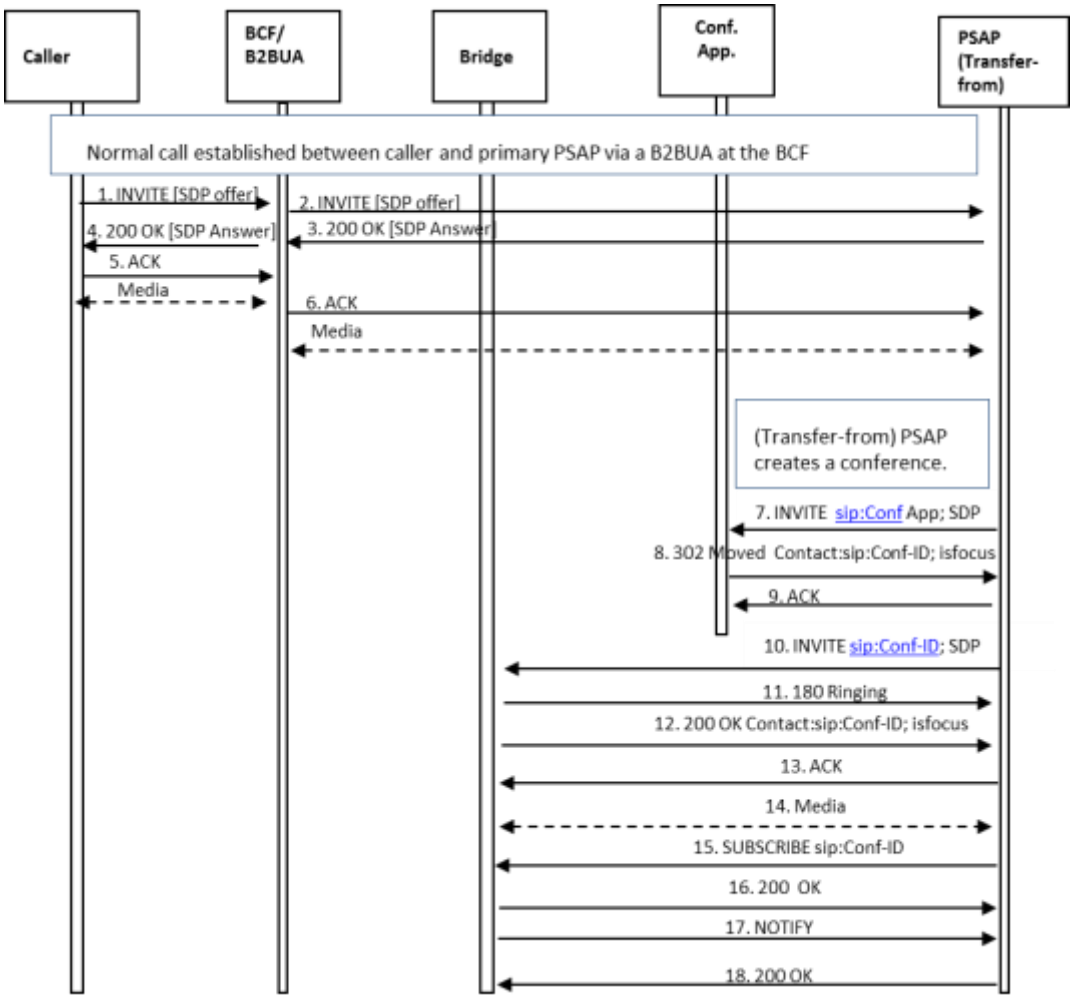


Figure 4-5 Ad Hoc Conference Call Flow Using SIP with B2BUA

1. The caller initiates an emergency session request by sending an INVITE message to the B2BUA. The INVITE contains callback information and a Geolocation header with caller location information. The Supported header field does not indicate support for the Replaces header field.

© Copyright 2011-2022 National Emergency Number Association, Inc.

2. The B2BUA forwards the INVITE to the ESRP (the URI in the Route header field, which should contain the "lr" parameter to avoid Request-URI rewriting) after changing the Contact header field to point to itself and changing the offer SDP media endpoint address and port to be itself. The INVITE includes a Supported header field indicating support for Replaces. The call proceeds through the ESInet/NGCS normally, and arrives at a PSAP.
3. The PSAP responds by returning a 200 OK message to the B2BUA, including its Contact URL and answer SDP in the response.
4. The B2BUA responds to the receipt of the 200 OK from the PSAP by sending a 200 OK message to the caller's device, changing the Contact to be itself and the answer SDP address and port to be itself.
5. The caller's device responds by sending an ACK to the B2BUA.

A media session is established between the caller and the B2BUA.

6. The B2BUA sends an ACK to the PSAP in response to receiving an ACK from the caller's device.

A media session is established between the B2BUA and the transfer-from PSAP.

7. The transfer-from PSAP creates a conference by first sending an INVITE with specified Media in the SDP to a Conference Application, using a URI that is known by/provisioned at the transfer-from PSAP.
8. The Conference Application responds by sending a 302 Moved message, which redirects the transfer-from PSAP to the conference bridge and provides the Conference URI that should be used for the conference.
9. The transfer-from PSAP acknowledges the receipt of the 302 Moved message.
10. The transfer-from PSAP generates an INVITE with specified Media in the SDP to establish a session with the conference bridge[43].
11. The conference bridge responds to the INVITE by returning a 180 Ringing message.
12. The conference bridge then returns a 200 OK message, and a media session is established between the transfer-from PSAP and the conference bridge.
13. The transfer-from PSAP returns an ACK message in response to the 200 OK.
14. Media. If SDP includes media-type specification for audio and/or video and/or RTT, then RTP media is exchanged. If SDP includes media-type specification for MSRP, then MSRP messages are exchanged.
15. through 18. Once the media session is established, the transfer-from PSAP subscribes to the conference associated with the URI obtained from the Contact header field provided in the 200 OK message from the conference bridge.

[43] Note that, based on RFC 4579, the messages sent in Steps 2, 8, 9, and 10 are optional and may not be exchanged if the conference application and the media server are the same.

© Copyright 2011-2022 National Emergency Number Association, Inc.

4.7.1.2.2 Transfer-from PSAP Asks Bridge to Invite the B2BUA to the Conference

This flow is based on Section 5.10 of RFC 4579 [39].

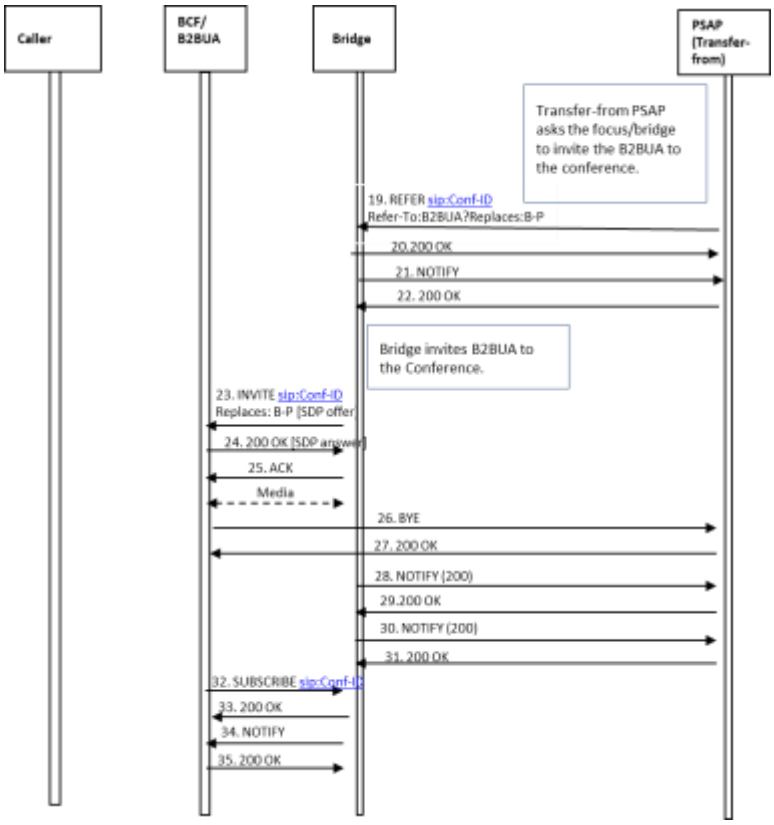


Figure 4-6 Transfer-from PSAP Asks Bridge to Invite the Caller/B2BUA to the Conference

19. After the transfer-from PSAP establishes the conference, it sends a REFER method to the conference bridge asking it to invite the caller/B2BUA to the conference. The REFER method contains an escaped Replaces header field value in the URI included in the Refer-To header field.
20. The bridge returns a 200 OK message to the transfer-from PSAP.
21. The bridge then returns a NOTIFY message, indicating the subscription state of the REFER request (i.e., active).
22. The transfer-from PSAP returns a 200 OK in response to the NOTIFY message.
23. The bridge invites the caller/B2BUA to the conference by sending an INVITE method containing the Conference URI and a Replaces header field that references the leg between the B2BUA and the transfer-from PSAP and an SDP offer.

© Copyright 2011-2022 National Emergency Number Association, Inc.

24. The INVITE arrives at the B2BUA. It does not forward the INVITE. Instead, it accepts the invitation by returning a 200 OK message containing an answer SDP with the media address and port of itself.
25. The bridge acknowledges receipt of the 200 OK message by returning an ACK.

A media session is established between the B2BUA and the bridge. The media session between the caller and the B2BUA is not affected. If SDP includes media-type specification for audio and/or video and/or RTT, then RTP media is exchanged. If SDP includes media-type specification for MSRP, then MSRP messages are exchanged.

26. The B2BUA releases the connection to the transfer-from PSAP by sending a BYE message.
27. The transfer-from PSAP responds by returning a 200 OK message.
28. The bridge sends a NOTIFY message to the transfer-from PSAP to provide REFER processing status.
29. The transfer-from PSAP responds by returning a 200 OK message.
30. The bridge sends a NOTIFY message to the transfer-from PSAP to provide updated status associated with the conference state.
31. The transfer-from PSAP responds by returning a 200 OK message.
32. The B2BUA subscribes to the conference associated with the Conference URI provided in the INVITE message from the bridge by sending a SUBSCRIBE message to the bridge. (Optional)
33. The bridge acknowledges the subscription request by sending a 200 OK message back to the B2BUA. (Optional)
34. The bridge then returns a NOTIFY message to the B2BUA to provide subscription status information. (Optional)
35. The B2BUA responds by returning a 200 OK message. (Optional)

© Copyright 2011-2022 National Emergency Number Association, Inc.

4.7.1.2.3 Transfer-to PSAP is Invited to the Conference

This flow is based on Section 5.5 of RFC 4579 [39]. There are no differences (other than step numbers) between this flow and the comparable flow in the no-B2BUA case.

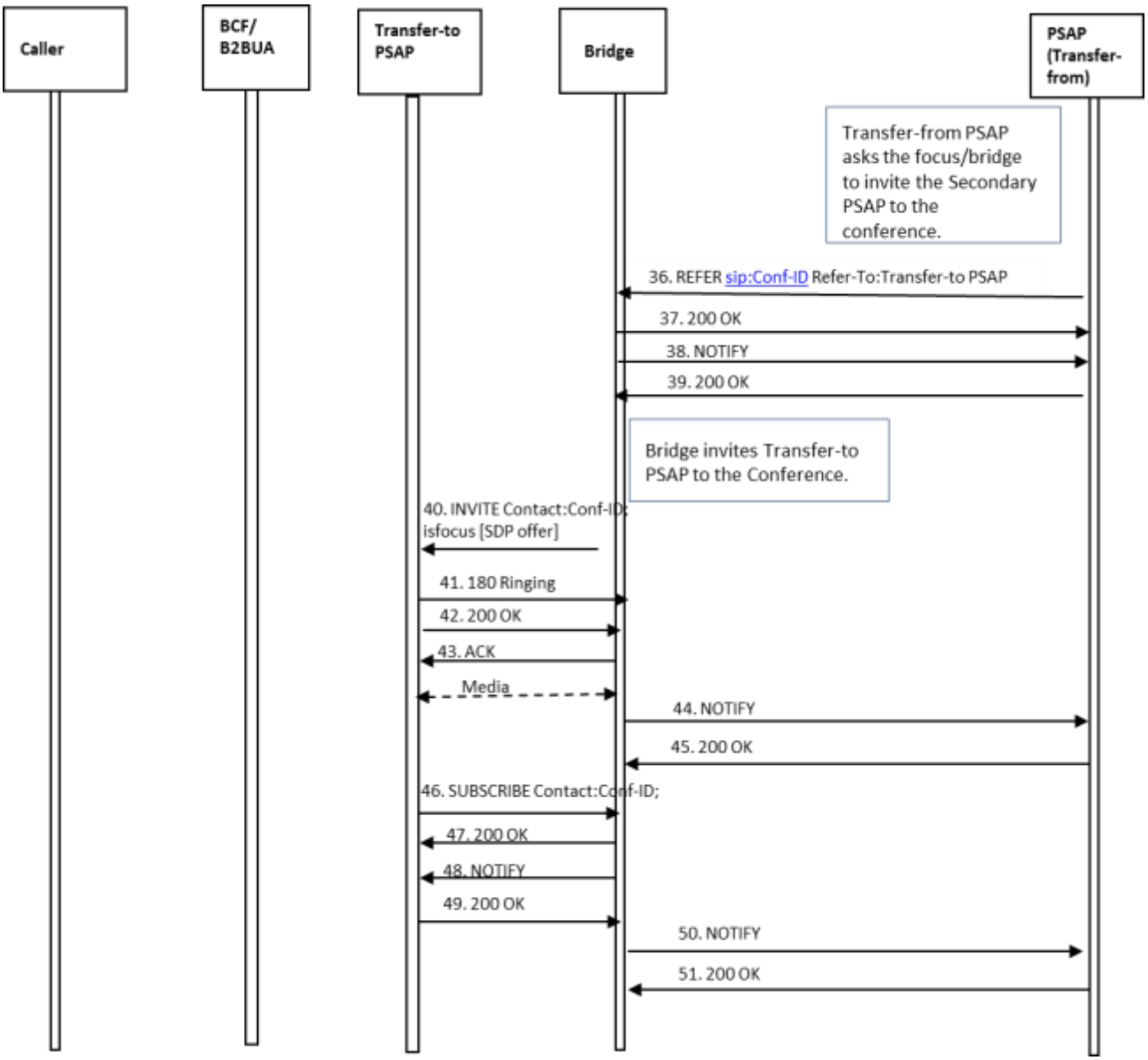


Figure 4-7 Transfer-to PSAP Invited to Conference

36. The transfer-from PSAP sends a REFER method to the conference bridge asking it to invite the transfer-to PSAP to the conference. The REFER method contains the Conference URI and a Refer-To header field that contains the URI of the transfer-to

© Copyright 2011-2022 National Emergency Number Association, Inc.

PSAP. The REFER method also contains an escaped Call-Info header field value containing a reference URI that points to the EIDO data structure and a purpose parameter of "emergency-eido".

37. The bridge returns a 200 OK message to the transfer-from PSAP.
38. The bridge then returns a NOTIFY message, indicating that subscription state of the REFER request (i.e., active).
39. The transfer-from PSAP returns a 200 OK in response to the NOTIFY message.
40. The bridge invites the transfer-to PSAP to the conference by sending an INVITE method containing the Conference URI and Contact header field that contains the conference URI, the 'isfocus' feature parameter, and an SDP offer. The INVITE contains the Call-Info header field containing a reference URI that points to the EIDO data structure and a purpose parameter of "emergency-eido".
41. The transfer-to PSAP UA responds by returning a 180 Ringing message to the bridge.
42. The transfer-to PSAP accepts the invitation by returning a 200 OK message.
43. The bridge acknowledges receipt of the 200 OK message by returning an ACK.

A media session is established between the transfer-to PSAP and the bridge. If SDP includes media-type specification for audio and/or video and/or RTT, then RTP media is exchanged. If SDP includes media-type specification for MSRP, then MSRP messages are exchanged.

44. The bridge returns a NOTIFY message to the transfer-from PSAP to provide updated status of the subscription associated with the REFER request.
45. The transfer-from PSAP responds to the NOTIFY message by returning a 200 OK message.
46. The transfer-to PSAP subscribes to the conference associated with the Conference URI provided in the INVITE message from the bridge by sending a SUBSCRIBE message to the bridge.
47. The bridge acknowledges the subscription request by sending a 200 OK message back to the transfer-to PSAP.
48. The bridge then returns a NOTIFY message to the transfer-to PSAP to provide subscription status information.
49. The transfer-to PSAP responds by returning a 200 OK message.
50. The bridge sends a NOTIFY message to the transfer-from PSAP providing updated status for the subscription associated with the REFER request.
51. The transfer-from PSAP responds to the NOTIFY message by returning a 200 OK message.

At this point the caller (via the B2BUA), transfer-from PSAP, and transfer-to PSAP are all participants in the conference.

© Copyright 2011-2022 National Emergency Number Association, Inc.

4.7.1.2.4 Transfer-from PSAP Drops Out of Conference; Transfer-to PSAP Completes Transfer

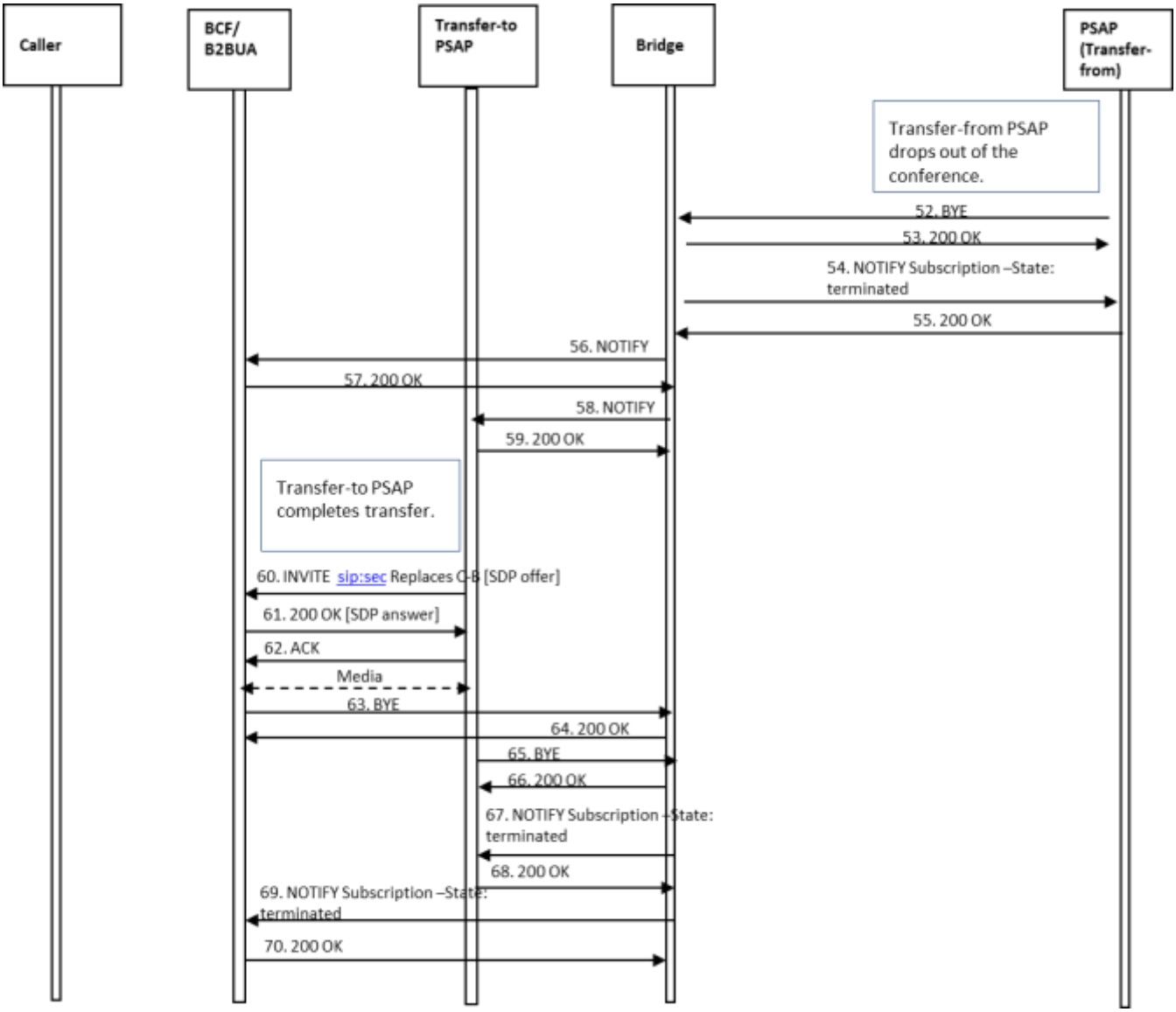


Figure 4-8 Transfer-from PSAP Drops, Transfer-to PSAP Completes Transfer

52. Upon determining that the emergency call transfer should be completed, the transfer-from PSAP disconnects from the call by sending a BYE message to the bridge.
53. The conference bridge responds by returning a 200 OK message.
54. The bridge then returns a NOTIFY message indicating that the subscription to the conference has been terminated.

© Copyright 2011-2022 National Emergency Number Association, Inc.

55. The transfer-from PSAP returns a 200 OK in response to the NOTIFY.
56. The bridge then returns a NOTIFY message to the B2BUA indicating that there has been a change to the subscription state. (Optional)
57. The B2BUA returns a 200 OK in response to the NOTIFY. (Optional)
58. The bridge returns a NOTIFY message to the transfer-to PSAP indicating that there has been a change to the subscription state.
59. The transfer-to PSAP returns a 200 OK in response to the NOTIFY.
60. Upon recognizing that the caller (via the B2BUA) and the transfer-to PSAP are the only remaining participants in the conference, the transfer-to PSAP completes the transfer by sending an INVITE with an SDP offer to the B2BUA requesting that they replace their connection to the bridge with a direct connection to the transfer-to PSAP. The transfer-to PSAP learns the URI of the B2BUA through the entity attribute in the endpoint section of the user's container in the conference NOTIFY from the bridge.
61. The B2BUA responds by returning a 200 OK message to the transfer-to PSAP.
62. The transfer-to PSAP returns an ACK in response to the 200 OK.

A media session is established between the transfer-to PSAP, the B2BUA (acting as a media relay), and the caller. If SDP includes media-type specification for audio and/or video and/or RTT, then RTP media is exchanged. If SDP includes media-type specification for MSRP, then MSRP messages are exchanged.

63. The B2BUA then sends a BYE to the bridge to terminate the session.
64. The bridge responds by sending the B2BUA a 200 OK message.
65. The transfer-to PSAP also terminates its session with the bridge by sending a BYE message to the bridge.
66. The bridge responds by sending a 200 OK message to the transfer-to PSAP.
67. The bridge then returns a NOTIFY message to the transfer-to PSAP indicating that the subscription to the conference has been terminated.
68. The transfer-to PSAP returns a 200 OK in response to the NOTIFY message.
69. The bridge sends a NOTIFY message to the B2BUA indicating that the subscription to the conference has been terminated. (Optional)
70. The B2BUA responds with a 200 OK message. (Optional)

At this point, the transfer is complete, and the caller (via the B2BUA) and the transfer-to PSAP are involved in a two-way call via the B2BUA.

4.7.1.2.5 Call Termination

If the caller terminates the call, it would send a BYE to the B2BUA. The B2BUA would forward it to the transfer-to PSAP after modifying the Contact to itself. The transfer-to PSAP would respond with a 200 OK which it would send to the B2BUA. The B2BUA would

© Copyright 2011-2022 National Emergency Number Association, Inc.

then forward the BYE to the caller. If the PSAP terminates the call, it would send a BYE to the B2BUA, which would forward it to the caller after modifying the Contact. The caller would respond to the BYE with a 200 OK which it would send to the B2BUA. The B2BUA would forward that to the PSAP. (Steps not shown.)

4.7.1.3 Route All Calls Via a Conference Aware UA

All incoming 9-1-1 calls are routed via a conference-aware UA. The conference-aware UA initially acts as a B2BUA but inserts an 'isfocus' parameter in the INVITE forwarded to the PSAP, and in the 200 OK forwarded to the caller, possibly rewriting the SDP. The caller remains on the conference-aware UA to which it was first routed (but see Section 4.9 below when transferring between ESInets). If the PSAP, or any other party, sends a REFER to the conference-aware UA, the conference-aware UA behaves as a normal bridge would. The call taker can add other parties to the bridge, other parties can add additional parties, parties can drop off the bridge, and the caller to bridge leg remains stable. There are options for how media is handled in this scenario. First, the initial call can be negotiated with the media flowing between the caller and the PSAP, with a media relay B2BUA in the path (in addition to the conference-aware UA) and no media mixer, or second, it can be negotiated with no media relay and a media mixer always in the path. In the second case, if a REFER is sent to the conference-aware UA when only two parties are on the call, the conference-aware UA re-INVITEs the parties, acting as a full bridge, and renegotiates the SDP to both parties to land on a media mixer. It then sends an INVITE to the transferred-to PSAP to add it to the bridge. If in the first case, the media was initially negotiated to a B2BUA acting as a media relay, the caller and transfer-from PSAP see no re-INVITE, and the conference-aware UA sends an INVITE to the transfer-to PSAP to add it to the bridge.

© Copyright 2011-2022 National Emergency Number Association, Inc.

4.7.1.3.1 Call Established Between Caller and PSAP Via Conference-Aware UA.

This example shows the conference-aware UA handling media at the outset (second case above).

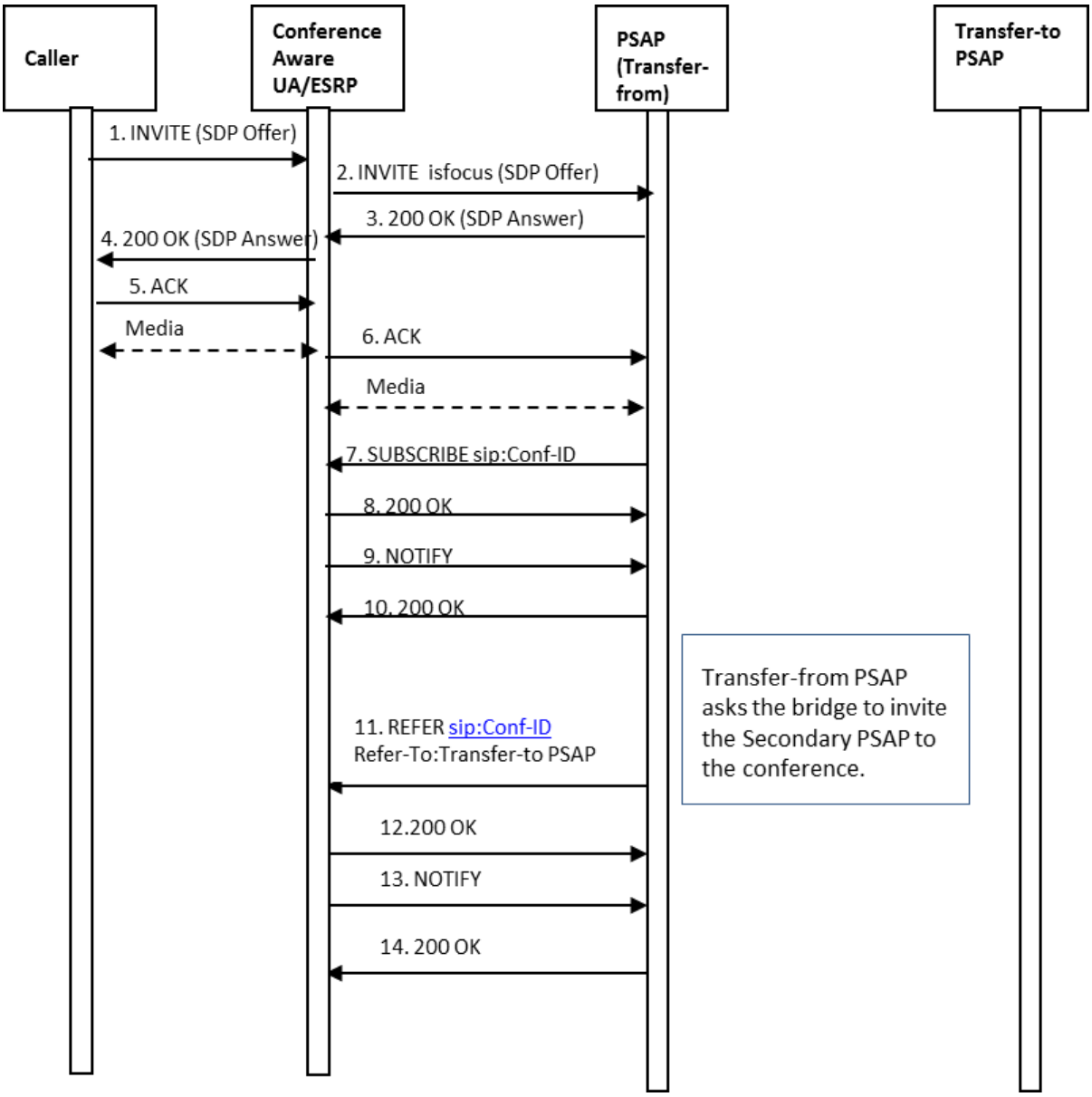


Figure 4-9 Call Established Via a Conference-aware UA

1. The caller initiates an emergency session request by sending an INVITE message to the conference-aware UA. The INVITE contains a Geolocation header field with caller location information.

© Copyright 2011-2022 National Emergency Number Association, Inc.

2. The conference-aware UA forwards the INVITE to the ESRP (the URI in the Route header field, which should contain the "lr" parameter to avoid Request-URI rewriting) after changing the Contact header field to point to itself, adding an 'isfocus' feature parameter and a ConferenceId as well as changing the offer SDP media endpoint address and port to be itself. The INVITE contains a Supported header field indicating support for Replaces. The call proceeds through the ESInet/NGCS normally and arrives at a PSAP.
3. The PSAP responds by returning a 200 OK message to the conference-aware UA, including its Contact URL and answer SDP in the response.
4. The conference-aware UA responds to the receipt of the 200 OK from the PSAP by sending a 200 OK message to the caller's device, changing the Contact to be itself and the answer SDP address and port to be itself, adding an 'isfocus' feature parameter and a Conference URI.
5. The caller's device responds by sending an ACK to the conference-aware UA.

A media session is established between the caller and the conference-aware UA.

6. The conference-aware UA sends an ACK to the PSAP in response to receiving an ACK from the caller's device.

A media session is established between the conference-aware UA and the PSAP. For both media legs, if SDP includes media-type specification for audio and/or video and/or RTT, then RTP media is exchanged. If SDP includes media-type specification for MSRP, then MSRP messages are exchanged.

7. Once the media session is established, the transfer-from PSAP sends a SUBSCRIBE message to the conference-aware UA to subscribe to the conference associated with the Conference URI identified when the conference was initially established with the conference-aware UA.
8. The conference-aware UA responds to the SUBSCRIBE message by returning a 200 OK message to the transfer-from PSAP.
9. The conference-aware UA then returns a NOTIFY message to the transfer-from PSAP to provide it with status information regarding the conference.
10. The transfer-from PSAP responds to the NOTIFY message by returning a 200 OK message.
11. The transfer-from PSAP sends a REFER method to the conference-aware UA asking it to invite the transfer-to PSAP to the conference. The REFER method contains the Conference URI and a Refer-To header field that contains the URI of the transfer-to PSAP. The REFER method also includes an escaped Call-Info header field in the Refer-To header field containing a reference URI that points to the EIDO data structure with a purpose parameter of "emergency-eido".
12. The conference-aware UA returns a 200 OK message to the transfer-from PSAP.

© Copyright 2011-2022 National Emergency Number Association, Inc.

13. The conference-aware UA then returns a NOTIFY message, indicating that subscription state of the REFER request (i.e., active).
14. The transfer-from PSAP returns a 200 OK in response to the NOTIFY message.

4.7.1.3.2 Conference-aware UA Invites the Transfer-to PSAP to the Conference

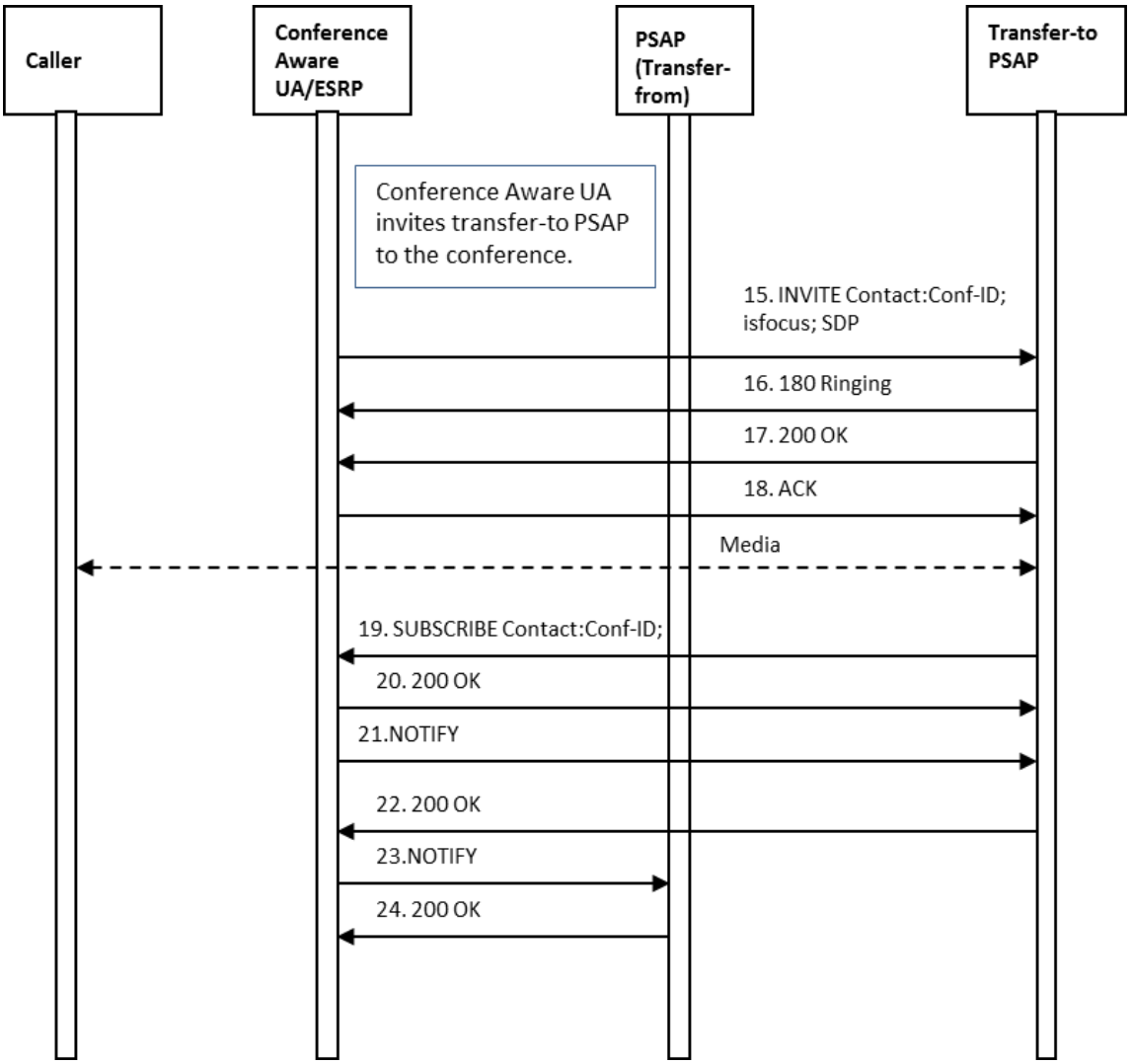


Figure 4-10 Secondary PSAP Invited to Conference

15. The conference-aware UA invites the transfer-to PSAP to the conference by sending an INVITE method containing the Conference URI and the 'isfocus' feature parameter. The INVITE also contains a Call-Info header field containing a reference

© Copyright 2011-2022 National Emergency Number Association, Inc.

URI that points to the EIDO data structure and a purpose parameter of "emergency-eido".

16. The transfer-to PSAP UA responds by returning a 180 Ringing message to the conference-aware UA.
17. The transfer-to PSAP accepts the invitation by returning a 200 OK message.
18. The conference-aware UA acknowledges receipt of the 200 OK message by returning an ACK.

A media session is established among the transfer-from PSAP, the transfer-to PSAP, and the caller.

19. The transfer-to PSAP subscribes to the conference associated with the Conference URI provided in the INVITE message from the conference-aware UA by sending a SUBSCRIBE message to the conference-aware UA.
20. The conference-aware UA acknowledges the subscription request by sending a 200 OK message back to the transfer-to PSAP.
21. The conference-aware UA then returns a NOTIFY message to the transfer-to PSAP to provide subscription status information.
22. The transfer-to PSAP responds by returning a 200 OK message.
23. The conference-aware UA sends a NOTIFY message to the transfer-from PSAP providing updated status for the subscription associated with the REFER request.
24. The transfer-from PSAP responds to the NOTIFY message by returning a 200 OK message.

At this point the caller, transfer-from PSAP, and transfer-to PSAP are all participants in the conference.

© Copyright 2011-2022 National Emergency Number Association, Inc.

4.7.1.3.3 Transfer-from PSAP Drops Out of Conference; Transfer-to PSAP Completes Transfer

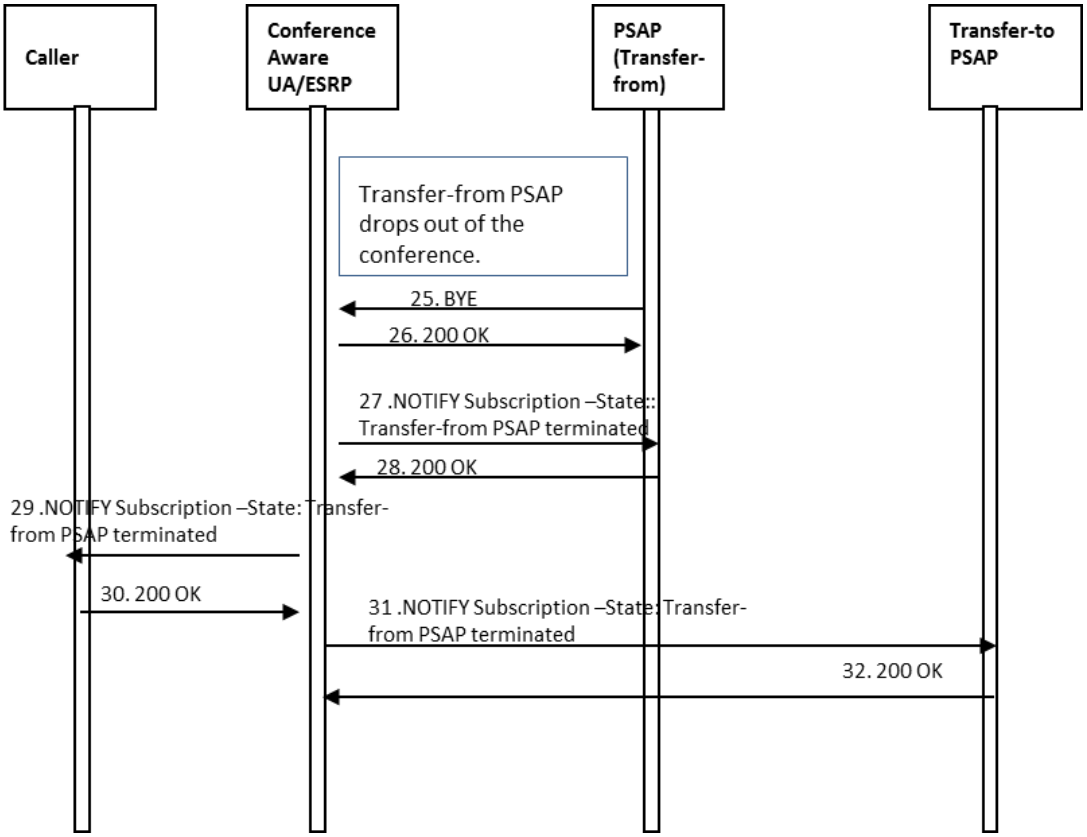


Figure 4-11 Transfer-from PSAP Drops, Transfer-to PSAP Completes Transfer

25. Upon determining that the emergency call transfer should be completed, the transfer-from PSAP disconnects from the call by sending a BYE message to the conference-aware UA.
26. The conference-aware UA responds by returning a 200 OK message.
27. The conference-aware UA then returns a NOTIFY message to the transfer-from PSAP indicating that the subscription to the conference has been terminated.
28. The transfer-from PSAP returns a 200 OK in response to the NOTIFY.
29. The conference-aware UA then returns a NOTIFY message to the caller indicating that there has been a change to the subscription state. (Optional)
30. The caller returns a 200 OK in response to the NOTIFY. (Optional)
31. The conference-aware UA returns a NOTIFY message to the transfer-to PSAP indicating that there has been a change to the subscription state.
32. The transfer-to PSAP returns a 200 OK in response to the NOTIFY.

© Copyright 2011-2022 National Emergency Number Association, Inc.

At this point, the transfer is complete. The caller and the transfer-to PSAP are involved in a two-way call via the conference-aware UA.

4.7.1.3.4 Transfer-to PSAP Terminates the Call

When the transfer-to PSAP determines that the call should be terminated, it will follow the flow illustrated below.

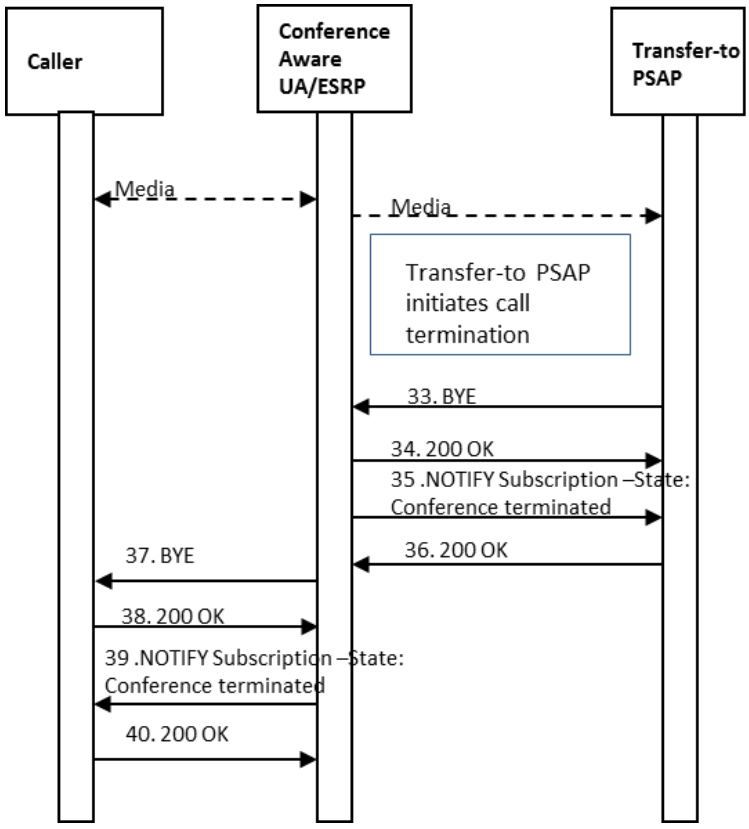


Figure 4-12 Transfer-to PSAP Terminates Call

33. The transfer-to PSAP initiates call termination by sending a BYE message to the conference-aware UA.
34. The conference-aware UA responds by returning a 200 OK message.
35. The conference-aware UA then returns a NOTIFY message to the transfer-to PSAP indicating that the subscription to the conference has been terminated.
36. The transfer-to PSAP returns a 200 OK in response to the NOTIFY.

At this point, the session between the bridge and the transfer-to PSAP is torn down.

37. The conference-aware UA sends a BYE message to the caller's device.

© Copyright 2011-2022 National Emergency Number Association, Inc.

38. through 40. The caller's device responds by returning a 200 OK message to the conference-aware UA.

At this point, the session between the caller and the conference-aware UA is torn down.

4.7.2 Blind Transfers

Blind Transfer involves transferring a call without communication with the recipient. It is also known as unsupervised transfer or cold transfer. As opposed to Bridging and Attended transfer (section 4.7), the transferring PSAP Telecommunicator is not in communication with the transfer-to PSAP Telecommunicator during the transferring process. This transfer operation generally follows the sequence as shown in RFC 3515 [19].

As noted in section 4.7, there are two methods of ESInet implementation. One method is termed "ad hoc" and is characterized by using a bridge only when it is needed during attended transferring or conferencing more than two parties. The other mechanism is "Route All Calls Via a Conference Aware UA". In this method, at least the signaling portion of a bridge is always in the call path. The implementation of blind transfer differs slightly between the methods. For a blind transfer in ESInets using the ad hoc method, the transferring PSAP SHALL NOT seize the bridge prior to initiating a blind transfer.

The transfer-from PSAP MUST send a REFER where the Request Line contains the caller information. The Refer-To header field MUST specify the transfer-to PSAP (or any other entity): for consistency with Bridging and Attended transfer, the transfer-from PSAP SHOULD include the EIDO URI in an escaped parameter in the Refer-To header field. See the example of the associated header fields in 4.7.1 above.

A REFER request implicitly establishes a subscription to the refer event as defined in RFC 3515 [19], but not regarding the conference as a whole. Once the REFER is successfully acknowledged with a 200 OK, the recipient of the REFER will send notifications of the status of the adding the target participant. It MAY send a notification containing a 100 Trying to indicate the transfer is pending. It MAY also send additional provisional messages, e.g. 183 Session Progress. It MUST send a 200 OK indicating that the party was successfully added. At this point the transferring PSAP MUST send a BYE to end its participation in the call. If the transferring PSAP receives an error code in the notification, e.g. 503 Service Unavailable, it MUST assume that the transfer did not occur, and MUST NOT terminate the call.

4.7.3 Premature abandonment of a transfer by the Primary PSAP

Normally an emergency call completes the entire consultative transfer operation described above. There are circumstances where, for example a 9-1-1 call turns out not to be an emergency call, in which case blind transfer as described in Section 4.7.2 is used. If for any

© Copyright 2011-2022 National Emergency Number Association, Inc.

reason a consultative transfer must be terminated early, the following procedures MUST be used.

A REFER request implicitly establishes a subscription to the refer event as defined in RFC 3515 [19], but not regarding the conference as a whole. Once the REFER is successfully acknowledged with a 200 OK, the recipient of the REFER will send notifications of the status of the adding the target participant. It MAY send a notification containing a 100 Trying to indicate the transfer is pending. It MAY also send additional provisional messages, e.g. 183 Session Progress. It MUST send a 200 OK indicating that the party was successfully added. At this point the transferring PSAP MUST send a BYE to end its participation in the call. If the transferring PSAP receives an error code in the notification, e.g. 503 Service Unavailable, it MUST assume that the transfer did not occur and MUST not terminate the call.

4.7.4 Passing Data to Agencies via Bridging

When another PSAP is bridged to a 9-1-1 call there are separate "legs" for each participant in the bridge. The 9-1-1 call itself terminates at the bridge, with the call taker and the transfer target (e.g., transfer-to PSAP) having separate legs into the bridge. When the transfer target receives the initial SIP transaction it is an INVITE from the bridge to establish a conference. It is critical that the transfer target receives (or has access to) the location of the original caller, as well as any Additional Data that the transferring PSAP call taker may have received during the processing of the emergency call or was generated by the call taker as a result of processing the incoming emergency call. Caller location information along with any Additional Data MUST be populated in an Emergency Incident Data Object (EIDO) structure (see Section 7 for further discussion of Additional Data structures). When an emergency call is transferred, the transferring PSAP will request that the bridge insert a reference to the EIDO via an embedded Call-Info header field with a URI that points to the EIDO data structure in the REFER method sent to the bridge, and a purpose parameter of "emergency-eido". See the example of the associated header fields in 4.7.1 above. The bridge MUST subsequently include this Call-Info header field in the INVITE it sends to the transfer target.

The EIDO MUST be passed by reference when the Call-Info header field contains a URL that, when dereferenced, yields the EIDO. While the EIDO normally could be passed by value (in which case the Call-Info header field in an INVITE would contain a Content Identifier URI and the body of the INVITE would contain the EIDO in a MIME type of Application/EmergencyCallData.eido+json), such a construct could not be invoked at the bridge by an embedded header field in the Refer-To from the transferring PSAP. To dereference the URI and obtain the EIDO, the recipient initiates an HTTPS: GET on the URI and the EIDO [111] is returned. The GET request MUST contain an 'Accept:' header field

© Copyright 2011-2022 National Emergency Number Association, Inc.

which specifies the MIME type assigned to EIDO (application/emergency.eido+json) and MUST include as a parameter a comma-delimited list of the major version(s) of the schema the client supports (for example 'Accept: application/emergency.eido+json;version="1,2,3"'). If the server can fulfil the request, the response MUST include one and only one EIDO instance in the body of the reply. The version of the EIDO instance must be the highest mutually compatible major version. The server SHOULD send the highest minor version it supports of that major version. The client MUST expect to receive an object derived from any minor version of the specified EIDO schema, including a higher minor version than it currently supports. The client MUST ignore any fields it does not understand. If the server does not support any of the major versions found in the 'Accept:' header field of the GET request, it MUST return a 406 Not Acceptable response.

The EIDO contains a snapshot of the state of the Incident, as known by the sending Agency at the time it was sent.

4.7.5 Interoperability Between Transfer Models

An NGCS service provider chooses to support one of the transfer models described above. Transfers within the ESInet will consistently use that model. See Section 4.9 for inter-ESInet transfers.

Note that the calling device can work with either model. With the Ad Hoc method, if the calling device supports the Replaces header field, it will receive an INVITE with Replaces as the transfer proceeds. If the Ad Hoc method is implemented and the calling device does not support the Replaces header, a B2BUA in the call path will receive an INVITE with Replaces, without any impact on the calling device. With the Route All Calls Via a Conference-aware UA model, the caller may encounter a re-INVITE with a change in media endpoints. It could notice that the initial call is answered with the conference indication (isfocus feature parameter), but it need not take any action as a result.

PSAPs MUST implement both transfer models. A particular deployment would use only one model, as determined by the NGCS operator. The model choice is made by provisioning at the PSAP.

4.7.6 Conference Bridging for MSRP Text

As mentioned above (in Section 4.7), bridges in NG9-1-1 support multimedia. This includes voice and/or text and/or video. All bridges enable multi-party conferences that can be used to perform transfers. For MSRP text, this is equally true, except that the text media streams are not mixed, and kept independent. This is accomplished via the use of the Common Profile for Instant Messaging (CPIM) (RFC 3860) [176] (RFC 3862) [177] extensions to SIP. As specified in RFC 7701 [123], SIP/MSRP session + CPIM based

© Copyright 2011-2022 National Emergency Number Association, Inc.

protocols allow each individual message of an MSRP session to be sent to a group of participants or privately to a specific participant.

The manner in which transfers are orchestrated is important. Transfers for voice communication can typically be divided into two approaches: Supervised /Attended or Non-supervised/Unattended. Sometimes these are also referred to as Hold/No Hold transfers. This section describes only the Supervised/Attended transfer scenario as applied to MSRP text sessions.

When an MSRP text session must be transferred, a conference is set up. For text, a conference consists of forwarding messages to one or more parties. The result is a conference within the text part of the bridge that is commonly referred to as a Chat Room, where complete messages from each participant are interleaved and labeled by the participant before being sent to other participants.

Because some user devices do not currently support CPIM, the NG9-1-1 conference bridge MUST emulate what a CPIM-enabled device would do to appropriately interwork (e.g., label) text from other participants. User interface issues of how associated with the way that this appears to the conference participants are out of scope for this document.

For MSRP text transfers, a text conference is initially established between the end user and the call taker using the same SIP call flows shown for voice. The CPIM protocol is then used for initiating a supervised transfer to a third participant (e.g., transfer-to PSAP). The text conference bridge supports "private" messaging for transfer coordination between the original call-taker and the transfer-to call-taker. The private messaging is kept out-of-view of the other participants. Once the transfer has been completed, new text messaging from all parties is visible within the text conference bridge based on "regular/public" CPIM enabled marking.

All ESInet/NGCS CPIM-enabled endpoints MUST implement the nickname negotiation feature of RFC 7701 [123] and offer a nickname. There is no mechanism that allows a user to use that nickname to contact the PSAP outside the current conversation.

SIP/MSRP session setup with CPIM is specified within the SDP of an INVITE message in the initial conference setup. All endpoints and media intermediaries within an ESInet/NGCS MUST support CPIM.

The NGCS includes a conference bridge that anchors the MSRP media. We refer to this generally as a text part of the conference bridge. The text part supports a multi-party "chat room" which is invoked by a SIP REFER as part of a text transfer request modeling an ad hoc conference call flow.

Note: An ad hoc transfer call flow involving MSRP may be provided in a future version of this document.

© Copyright 2011-2022 National Emergency Number Association, Inc.

4.8 Media Mixing

Identification of participants uses RTCP SDES CNAME and NAME reports per Section 6.5 of RFC 3550 [11]. The RTCP SDES report SHOULD contain identification of the source represented by the CSRC identifier. This identification MUST contain the CNAME field and MAY contain the NAME field and other defined fields of the SDES report. All NG9-1-1 implementations MUST supply identity information in this manner to the bridge. Callers SHOULD do so. The bridge MUST convey SDES information received from the sources of the session members. When such information is not available, the focus UA MUST compose CSRC, CNAME, and NAME information from available information from the SIP session (From and P-A-I) with the participant.

All session participants observe the incoming RTP packets and make note of what source they came from in order to be able to present text in a way that identifies the source where possible.

4.8.1 Mixing of Real-time Text

Section 4.8 describes inter-PSAP conferencing capabilities involving a media mixer responsible for mixing media streams from the caller, the transferor and the transfer-to target. Mixing of audio and video is well understood. Mixing of Instant Messages is accomplished with "group chat" functions. Mixing of real-time text has, however originally been implemented without multi-party support; these implementations have been "multi-party unaware".

Receivers of true multi-party real-time text must actively identify the source of each received text block and place it appropriately for presentation. Multi-party unaware endpoints do not have that functionality. Therefore, there is a need to introduce a negotiation between mixers and endpoints for multi-party RTT capability so that mixers will send truly mixed real-time text only to endpoints who understand the mixed format. Endpoints without capability for true multi-party mixing of RTT are supported with a lower functionality providing a simulated grouped view of multi-party real-time text.

Transport of real-time text is originally specified in RFC 4103 [85]. Multi-party handling for real-time text is described in RFC 9071 [219], which updates RFC 4103. The Mixer function of the Bridge MUST implement these mechanisms for both multi-party aware and multi-party unaware end devices.

Negotiation of multi-party awareness SHALL be performed by mixers and endpoints at session initiation and modification. If both parties declare multi-party capability awareness, the mixer SHALL apply the mixing procedures for multi-party awareness as defined in RFC 9071 [219]. In all other cases, the mixer SHALL apply the limited functionality mixing procedures for multi-party unaware participants as defined in RFC 9071 [219].

© Copyright 2011-2022 National Emergency Number Association, Inc.

Using the original procedures in RFC 4103 [85] in a single stream in multi-party sessions results in text delays that would impede the real-time experience when two or more participants send text simultaneously. The multi-party extension defined in RFC 9071 [219] enables a number of participants to send text simultaneously while maintaining real-time experience for the receivers.

As specified in RFC 4103 [85] and in RFC 9071 [219], RTT is typically sent with two repetitions in order to reduce the risk of losing text in the case of packet loss. This applies for both multi-party aware and multi-party unaware cases.

The receiving endpoint with presentation functions, which has completed the negotiation for multi-party RTT awareness, SHALL use the source information to present text from the different sources separated in readable groups placed in an approximate relative time order. This way, new text from a number of different sources can be received and presented simultaneously or with negligible delay.

The format for multi-party RTT specified in RFC 9071 [219] is suitable also for two-party calls.

For the case when the multi-party awareness negotiation was unsuccessful, the mixer SHALL compose a simulated limited multi-party RTT view suitable for presentation. With this presentation, the time for source switching is depending on the actions of the users. In order to expedite source switching, a user can, for example, end its turn with a new line.

Mixers SHALL be capable of handling both multi-party aware and multi-party unaware endpoints in the same multi-party session.

4.9 Inter-ESInet Transfers

Most transfers will be between PSAPs within an ESInet and will implement a consistent model. However, there will occasionally be a requirement to transfer from an Upstream ESInet, serving the Upstream (transfer-from) PSAP to a Downstream ESInet, serving the Downstream (transfer-to) PSAP and the models implemented on both sides of the transfer may not be the same. The principles that guided the requirements of this section are:

1. Transfers between any PSAPs anywhere must be possible, and any differences in the transfer methods used by the Upstream ESInet vs. the Downstream ESInet should be transparent to the Downstream PSAP.
2. The complexity of the inter-ESInet transfer is placed primarily on the bridge/conference-aware UA and PSAP behavior is dictated by the SIP signaling delivered by the ESInet provider.
3. Once a transfer completes, it is desirable that resources in the Upstream ESInet no longer be engaged. This is especially true of media mixer resources. A B2BUA in the

© Copyright 2011-2022 National Emergency Number Association, Inc.

signaling path to support calling devices that do not implement the Replaces header field could be an exception.

4. Whenever possible, media "tromboning[44]" is to be avoided. For example, a wildly incorrectly routed call from New York that is initially answered at a PSAP in California and subsequently transferred to the correct New York PSAP should not have its media routed from New York to California and back to New York following completion of the transfer.

With two models, there are four possibilities.

- Upstream Ad Hoc Method to Downstream Ad Hoc Method
- Upstream Route All Calls Via a Conference-aware UA Method to Downstream Ad Hoc Method
- Upstream Ad Hoc Method to Downstream Route All Calls Via a Conference-aware UA Method
- Upstream Route All Calls Via a Conference-aware UA Method to Downstream Route All Calls Via a Conference-aware UA Method

4.9.1 Upstream Ad Hoc Method to Downstream Ad Hoc Method

The Upstream Ad Hoc method to Downstream Ad Hoc method is the most straightforward: the sequence in Sections 4.7.1.1 or 4.7.1.2 will work without change. Note that a B2BUA that anchors media would have the effect of tromboning the media, which is undesirable. The PSAP in the Downstream ESInet may subscribe to the Upstream conference bridge. Note that the Upstream PSAP is provisioned with the URL of its local conference bridge and if the Downstream PSAP initiates a transfer or conference while the conference is still active, it will use the Upstream bridge. If the Upstream PSAP drops from the conference, the Downstream PSAP will receive a notification. The Downstream PSAP may then send an INVITE with Replaces to reconfigure the media to remove the Upstream conference bridge. If the Downstream PSAP initiates a conference after the Upstream conference bridge is removed (e.g., the Upstream PSAP dropped), it will use its local bridge and not the bridge involved in the initial transfer.

4.9.2 Upstream Route All Calls Via a Conference Aware UA Method to Downstream Ad Hoc Method

The transfer in this case starts exactly as in Section 4.7.1.3.2. The Downstream PSAP MAY subscribe to the Upstream conference-aware UA to learn the identity of the conference

[44] Tromboning is where RTP media traffic originates at a certain point and follows a path out into the network and back to a destination close to where the RTP traffic originated.

© Copyright 2011-2022 National Emergency Number Association, Inc.

participants and changes in the state of the conference. If the Upstream PSAP drops, the Downstream PSAP will receive a NOTIFY to that effect. The Downstream PSAP MAY send an INVITE with Replaces toward the caller (which it learns from the conference roster) to reconfigure the call to remove the Upstream conference-aware UA. The caller/ingress BCF in the Upstream ESInet MAY return a "not supported" because the Upstream ESInet may not be configured to remove the conference-aware UA from the conference. In this case, the Downstream PSAP continues to use the Upstream bridge to perform any subsequent bridge/attended transfer operations. That is, the Downstream PSAP completes the sequence as described in Section 4.7.1.3.3, Steps 25 to 32.

If the Upstream ingress BCF is configured to support INVITE with Replaces, it will accept the INVITE with Replaces from the Downstream PSAP and send a BYE to the Upstream conference-aware UA. If the Downstream PSAP initiated a conference after the Upstream conference-aware UA is removed (e.g. the Upstream PSAP dropped), it will use its local bridge and not the bridge involved in the initial transfer. The sequence will be as described in Section 4.7.1.2.4, Steps 36 to 51.

4.9.3 Upstream Ad Hoc Method to Downstream Route All Calls Via a Conference-aware UA Method

The Downstream ESInets that implement Route All Calls Via a Conference-aware UA make use of a mechanism whereby the conference-aware UA in the Downstream ESInet acts as a B2BUA for all legs of a conference in the Upstream ESInet that terminate in the Downstream ESInet. This means that the Contact header which reflects the Upstream conference server, and the Conference ID, will be changed to reflect the Downstream conference-aware UA and Conference ID in the INVITE that is sent to the Downstream PSAP. The Downstream PSAP may subscribe to its local conference-aware UA, which may in turn subscribe to the Upstream conference server. If the Upstream PSAP drops, the NOTIFY will be sent by the Upstream conference server to the Downstream conference-aware UA, which will forward it to the Downstream PSAP. However, while the NOTIFY will be sent to the Downstream PSAP, there will be no attempt to reconfigure the media (i.e., the Downstream UA will not send an INVITE with Replaces). Regardless of whether the conference is active or the Upstream PSAP has dropped, if the Downstream PSAP adds another party it will use its local Downstream conference-aware UA.

At the completion of a transfer in which only the caller and the transfer-to PSAP remain in the conference, the Downstream conference-aware UA takes over the call, meaning it Replaces the connection between the caller (or a B2BUA in the path from the caller) and the transfer-from PSAP's bridge with a connection between the caller/B2BUA and itself. The B2BUA in the Upstream ESInet may need to remain in place if the calling device does not

© Copyright 2011-2022 National Emergency Number Association, Inc.

support Replaces. The downstream bridge MUST release the upstream bridge resources when no active call legs in the Upstream ESInet remain.

The initial sequence is the same as that in Sections 4.7.1.1 or 4.7.1.2 depending on whether a B2BUA is in the path). The remaining sequences associated with this inter-ESInet transfer configuration are described below.

4.9.3.1 Secondary PSAP is Invited to the Conference

1. The transfer-from PSAP in the Upstream ESInet sends a REFER method to its conference bridge asking it to invite the transfer-to PSAP to the conference, where the transfer-to PSAP is hosted in a Downstream ESInet. The REFER method contains the Upstream Conf-ID and a Refer-To header field that contains the URI of the transfer-to PSAP. The REFER method also contains an escaped Call-Info header field containing a reference URI that points to the EIDO data structure and a purpose parameter of "emergency-eido".
2. The Upstream conference-aware UA returns a 200 OK message to the Upstream/ transfer-from PSAP.
3. The Upstream conference-aware UA then returns a NOTIFY message, indicating that subscription state of the REFER request (i.e., active).
4. The Upstream/transfer-from PSAP returns a 200 OK in response to the NOTIFY message.
5. The Upstream conference-aware UA invites the Downstream/transfer-to PSAP to the conference by sending an INVITE method with SDP containing the Upstream Conf-ID and Contact header field that contains the conference URI and the 'isfocus' feature parameter. The INVITE contains the Call-Info header field containing a reference URI that points to the EIDO data structure and a purpose parameter of "emergency-eido". The URL obtained from the ECRF or other mechanisms for the Downstream/transfer-to PSAP is chosen to route to the conference-aware UA in the Downstream ESInet.
6. The Downstream conference-aware UA acts as a B2BUA, forwarding the INVITE to the Downstream/transfer-to PSAP after modifying the Contact to itself and substituting the Downstream Conf-Id it creates for the conference.
7. The Downstream PSAP UA responds by returning a 180 Ringing message to the conference aware UA.
8. The Downstream conference-aware UA forwards the 180 Ringing to the Upstream conference-aware UA after changing the Contact address to itself.
9. The Downstream/transfer-to PSAP accepts the invitation by returning a 200 OK message to the conference-aware UA.
10. The Downstream conference-aware UA forwards the 200 OK to the Upstream conference-aware UA after changing the Contact address to itself.

© Copyright 2011-2022 National Emergency Number Association, Inc.

11. The Upstream conference-aware UA acknowledges receipt of the 200 OK message by returning an ACK to the Downstream conference-aware UA.
12. The Downstream conference-aware UA forwards the ACK to the Downstream/transfer-to PSAP.

Depending upon implementation, a media session is established among the Downstream/transfer-to PSAP, the Upstream conference-aware UA, and the Downstream conference-aware UA. Optionally, the Downstream conference-aware UA is not placed in the media path until an additional action (e.g., the *Downstream/transfer-to PSAP requests to add another party) occurs. If SDP includes media-type specification for audio and/or video and/or RTT, then RTP media is exchanged. If SDP includes media-type specification for MSRP, then MSRP messages are exchanged.*

13. The Upstream conference-aware UA returns a NOTIFY message to the Upstream/transfer-from PSAP to provide updated status of the subscription associated with the REFER request.
14. The Upstream/transfer-from PSAP responds to the NOTIFY message by returning a 200 OK message.
15. The Downstream conference-aware UA subscribes to the Upstream conference-aware UA associated with the Conf-ID provided in the INVITE message from the conference-aware UA by sending a SUBSCRIBE message to it.
16. The Upstream conference-aware UA acknowledges the subscription request by sending a 200 OK message back to the Downstream conference-aware UA.
17. The Upstream conference-aware UA then returns a NOTIFY message to the Downstream conference-aware UA to provide subscription status information.
18. The Downstream conference-aware UA responds by returning a 200 OK message.
19. The Downstream/transfer-to PSAP subscribes to the Downstream conference-aware UA associated with the Conf-ID provided in the INVITE message from the Downstream conference-aware UA by sending a SUBSCRIBE message to the Downstream conference-aware UA.
20. The Downstream conference-aware UA acknowledges the subscription request by sending a 200 OK message back to the Downstream/transfer-to PSAP.
21. The Downstream conference-aware UA then returns a NOTIFY message to the Downstream/transfer-to PSAP to provide subscription status information obtained from the bridge, modified appropriately.
22. The Downstream/transfer-to PSAP responds by returning a 200 OK message.
23. The Upstream conference-aware UA sends a NOTIFY message to the Upstream/transfer-from PSAP providing updated status for the subscription associated with the REFER request.

© Copyright 2011-2022 National Emergency Number Association, Inc.

24. The Upstream/transfer-from PSAP responds to the NOTIFY message by returning a 200 OK message.

At this point the caller, Upstream/transfer-from PSAP, and Downstream/transfer-to PSAP (via the Upstream and Downstream conference aware-UAs) are all participants in the conference.

4.9.3.2 Upstream PSAP Drops Out of Conference; Downstream PSAP Completes Transfer

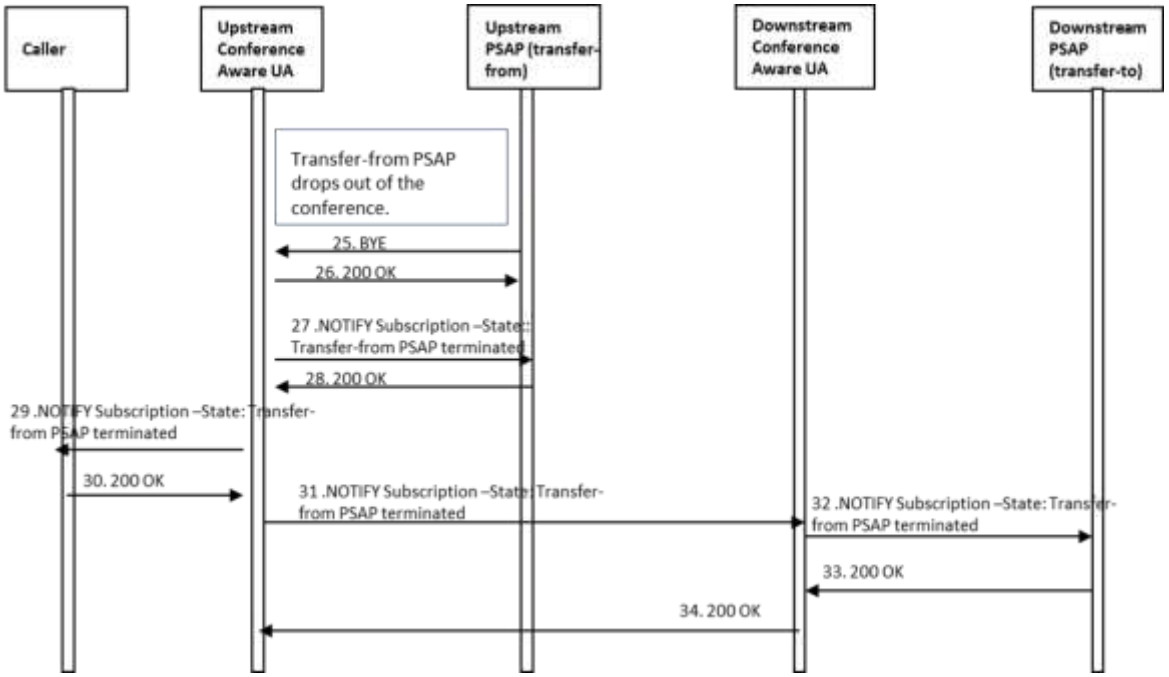


Figure 4-13 Upstream PSAP Drops, Downstream PSAP Completes Transfer

25. Upon determining that the emergency call transfer should be completed, the Upstream/transfer-from PSAP disconnects from the call by sending a BYE message to the Upstream conference-aware UA.
26. The Upstream conference-aware UA responds by returning a 200 OK message.
27. The Upstream conference-aware UA then returns a NOTIFY message indicating that the subscription to the conference has been terminated.
28. The Upstream/transfer-from PSAP returns a 200 OK in response to the NOTIFY.
29. The Upstream conference-aware UA may send a NOTIFY message to the caller indicating that there has been a change to the subscription state. (Optional)
30. The caller returns a 200 OK in response to the NOTIFY. (Optional)
31. The Upstream conference-aware UA sends a NOTIFY message to the Downstream conference-aware UA indicating that there has been a change to the subscription state.

© Copyright 2011-2022 National Emergency Number Association, Inc.

32. The Downstream conference-aware UA sends a NOTIFY message to the Downstream/transfer-to PSAP indicating the state change.
33. The Downstream/transfer-to PSAP returns a 200 OK in response to the NOTIFY, however it takes no other action (i.e., it does not send an INVITE with replaces).
34. The Downstream conference-aware UA forwards the 200 OK to the Upstream conference-aware UA.

At this point, the Upstream/transfer-from PSAP has dropped and the caller and the Downstream/transfer-to PSAP are communicating via the Upstream and Downstream conference-aware UAs.

4.9.4 Upstream Route All Calls Via a Conference Aware UA Method to Downstream Route All Calls Via a Conference Aware UA Method

The sequence for this case is very similar to the prior sequence. The Upstream and Downstream ESInets that implement Route All Calls Via a Conference Aware UA make use of a mechanism whereby the conference aware UA acts as a B2BUA for all legs of a conference in their ESInet. This means that the Upstream isfocus will be changed to the Downstream isfocus in the INVITE that is sent to the Downstream PSAP. The Downstream PSAP may subscribe to its local conference aware UA, which may in turn subscribe to the Upstream conference aware UA. If the Upstream PSAP drops, the NOTIFY will be sent by the Upstream conference aware UA to the Downstream conference aware UA, which will forward it to the Downstream PSAP. The NOTIFY will be sent to the Downstream PSAP, but there will be no attempt to reconfigure the media (i.e., the Downstream UA will not send an INVITE with Replaces). Regardless of whether the conference initiated by the Upstream PSAP is still active or in which the Upstream PSAP has dropped, if the Downstream PSAP adds another party it will use its local Downstream conference aware UA.

The initial sequence is the same as that in Sections 4.7.1.3.1. The remaining sequences for this inter-ESInet transfer configuration are described below.

4.9.4.1 Downstream PSAP is Invited to the Conference

1. The Upstream/transfer-from PSAP sends a REFER method to the Upstream conference aware UA asking it to invite the Downstream/transfer-to PSAP to the conference. The REFER method contains the Conf-ID and a Refer-To header field that contains the URI of the Downstream/transfer-to PSAP. The REFER method also contains an escaped Call-Info header field containing a reference URI that points to the EIDO data structure and a purpose parameter of "emergency-eido".
2. The Upstream conference aware UA returns a 200 OK message to the Upstream/transfer-from PSAP.

© Copyright 2011-2022 National Emergency Number Association, Inc.

3. The Upstream conference aware UA then returns a NOTIFY message, indicating that subscription state of the REFER request (i.e., active).
4. The Upstream/transfer-from PSAP returns a 200 OK in response to the NOTIFY message.
5. The Upstream conference aware UA invites the Downstream/transfer-to PSAP to the conference by sending an INVITE method with SDP that includes: the Conf-ID, a Contact header field that contains the conference URI, the 'isfocus' feature parameter, and a Call-Info header field that contains a reference URI pointing to the EIDO data structure along with a purpose parameter of "emergency-eido". The URL obtained from the ECRF or other mechanisms for the Downstream/transfer-to PSAP is chosen to route to the Downstream conference aware UA in the transfer-to ESInet.
6. The Downstream conference aware UA acts as a B2BUA, forwarding the INVITE to the Downstream/transfer-to PSAP after modifying the Contact to itself and substituting a Conf-Id it creates for the conference.
7. The Downstream PSAP UA responds by returning a 180 Ringing message to the downstream conference aware UA.
8. The Downstream conference aware UA forwards the 180 Ringing to the Upstream conference aware UA after changing the Contact address to itself.
9. The Downstream/transfer-to PSAP accepts the invitation by returning a 200 OK message to the Downstream conference aware UA.
10. The Downstream conference aware UA forwards the 200 OK to the Upstream conference aware UA after changing the Contact address to itself.
11. The Upstream conference aware UA acknowledges receipt of the 200 OK message by returning an ACK to the Downstream conference aware UA.
12. The Downstream conference aware UA forwards the ACK to the Downstream/transfer-to PSAP.

A media session is established between the Downstream/transfer-to PSAP and the media mixer in the primary conference aware UA. If SDP includes media-type specification for audio and/or video and/or RTT, then RTP media is exchanged. If SDP includes media-type specification for MSRP, then MSRP messages are exchanged.

13. The Upstream conference aware UA returns a NOTIFY message to the Upstream/transfer-from PSAP to provide updated status of the subscription associated with the REFER request.
14. The Upstream/transfer-from PSAP responds to the NOTIFY message by returning a 200 OK message.
15. The Downstream conference aware UA subscribes to the conference associated with the Conf-ID provided in the INVITE message from the Upstream conference aware

© Copyright 2011-2022 National Emergency Number Association, Inc.

UA by sending a SUBSCRIBE message to the Upstream conference aware UA. Note that the Downstream conference aware UA always subscribes to the event package even if the Downstream/transfer-to PSAP does not subscribe.

16. The Upstream conference aware UA acknowledges the subscription request by sending a 200 OK message back to the Downstream conference aware UA.
17. The Upstream conference aware UA then returns a NOTIFY message to the Downstream conference aware UA to provide subscription status information.
18. The Downstream conference aware UA responds by returning a 200 OK message.
19. The Downstream/transfer-to PSAP subscribes to the conference associated with the Conf-ID provided in the INVITE message from the Downstream conference aware UA by sending a SUBSCRIBE message to the Downstream conference aware UA.
20. The Downstream conference aware UA acknowledges the subscription request by sending a 200 OK message back to the Downstream/transfer-to PSAP.
21. The Downstream conference aware UA then returns a NOTIFY message to the Downstream/transfer-to PSAP to provide subscription status information obtained from the Upstream conference aware UA, modified appropriately.
22. The Downstream/transfer-to PSAP responds by returning a 200 OK message.
23. The Upstream conference aware UA sends a NOTIFY message to the Upstream/transfer-from PSAP providing updated status for the subscription associated with the REFER request.
24. The Upstream/transfer-from PSAP responds to the NOTIFY message by returning a 200 OK message.

At this point the caller, Upstream/transfer-from PSAP, and Downstream/transfer-to PSAP (via the conference aware UA) are all participants in the conference.

© Copyright 2011-2022 National Emergency Number Association, Inc.

4.9.4.2 Upstream PSAP Drops Out of Conference; Downstream PSAP Completes Transfer

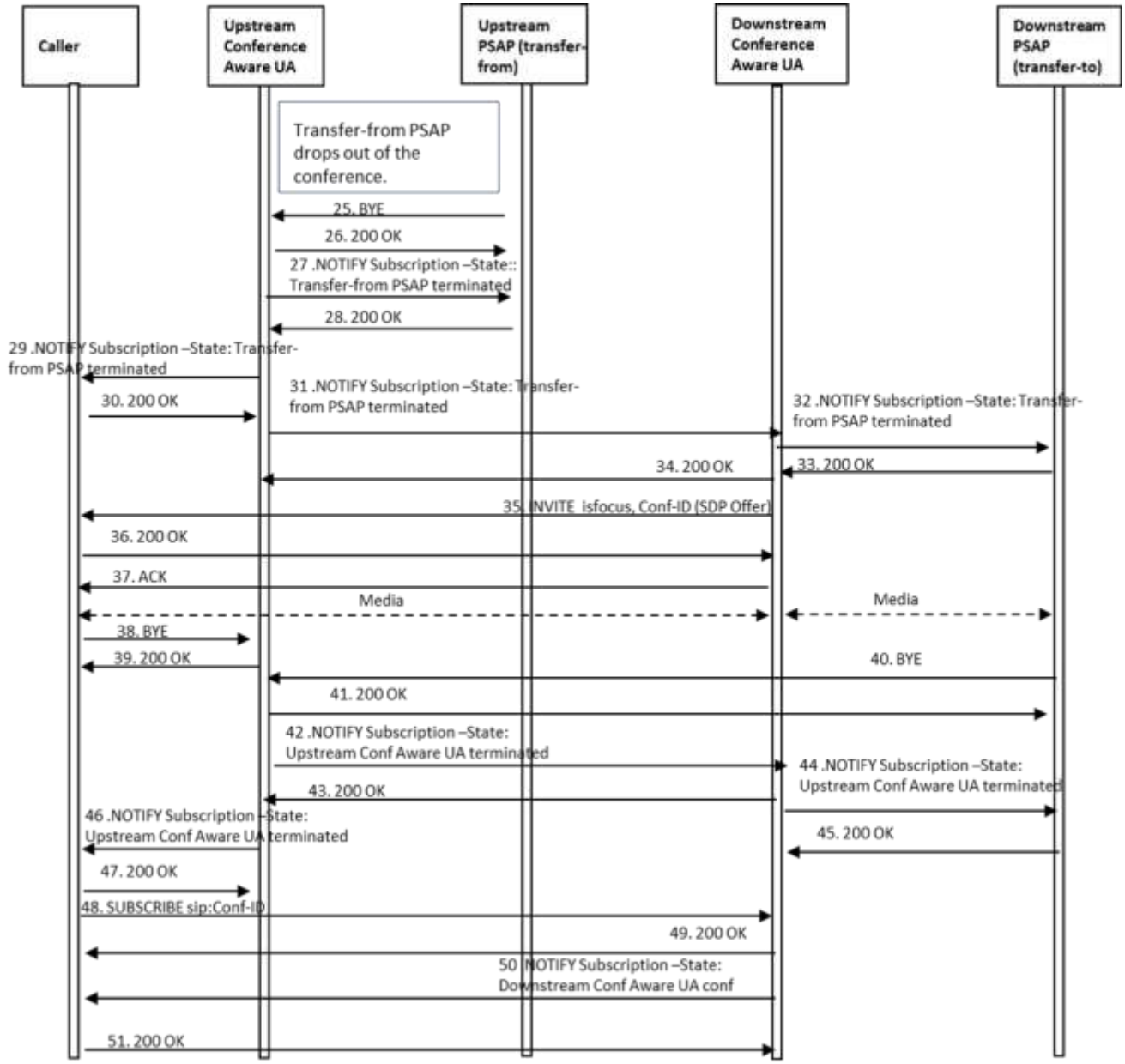


Figure 4-14 Primary PSAP Drops, Secondary Completes Transfer

25. Upon determining that the emergency call transfer should be completed, the Upstream/transfer-from PSAP disconnects from the call by sending a BYE message to the Upstream conference aware UA.

© Copyright 2011-2022 National Emergency Number Association, Inc.

26. The Upstream conference aware UA responds by returning a 200 OK message.
27. The Upstream conference aware UA then returns a NOTIFY message indicating that the subscription to the conference has been terminated.
28. The Upstream/transfer-from PSAP returns a 200 OK in response to the NOTIFY.
29. The Upstream conference aware UA then returns a NOTIFY message to the caller indicating that there has been a change to the subscription state. (Optional)
30. The caller returns a 200 OK in response to the NOTIFY. (Optional)
31. The Upstream conference aware UA sends a NOTIFY message to the Downstream conference aware UA indicating that there has been a change to the subscription state.
32. The Downstream conference aware UA sends a NOTIFY message to the Downstream/transfer-to PSAP indicating the state change, however the PSAP takes no further action (e.g., doesn't send an INVITE with replaces).
33. The Downstream/transfer-to PSAP returns a 200 OK in response to the NOTIFY.
34. The Downstream conference aware UA forwards the 200 OK to the Upstream conference aware UA.
35. Upon recognizing that the caller and the Downstream/transfer-to PSAP (via the Downstream conference aware UA) are the only remaining participants in the conference, the Downstream conference aware UA completes the transfer by sending an INVITE with Replaces, SDP, an isfocus feature parameter, and the conference aware UA's Conf-ID to the caller/B2BUA requesting that they replace their connection to the bridge with a connection to the Downstream conference aware UA. The Downstream conference aware UA learns the URI of the caller through the entity attribute in the endpoint section of the user's container in the conference NOTIFY from the Upstream conference aware UA.
36. The caller responds by returning a 200 OK message to the Downstream conference aware UA.
37. The Downstream conference aware UA returns an ACK in response to the 200 OK.

A media session is established between the Downstream/transfer-to PSAP and the caller using the Downstream conference aware UA's media mixer. If SDP includes media-type specification for audio and/or video and/or RTT, then RTP media is exchanged. If SDP includes media-type specification for MSRP, then MSRP messages are exchanged.

38. The caller then sends a BYE to the Upstream conference aware UA to terminate the session.
39. The Upstream conference aware UA responds by sending the caller a 200 OK message.

© Copyright 2011-2022 National Emergency Number Association, Inc.

40. The Downstream conference aware UA also terminates its session with the Upstream conference aware UA by sending a BYE message to the Upstream conference aware UA.
41. The Upstream conference aware UA responds by sending a 200 OK message to the Downstream conference aware UA.
42. The Upstream conference aware UA then returns a NOTIFY message to the Downstream conference aware UA indicating that the subscription to the conference has been terminated.
43. The Downstream conference aware UA returns a 200 OK in response to the NOTIFY message.
44. The Downstream conference aware UA then returns a NOTIFY message to the Downstream/transfer-to PSAP indicating that the conference state has changed.
45. The Downstream conference aware UA returns a 200 OK in response to the NOTIFY message.
46. The Upstream conference aware UA sends a NOTIFY message to the caller indicating that the subscription to its conference has been terminated. (Optional)
47. The caller responds with a 200 OK message. (Optional)
48. The caller subscribes to the conference associated with the Conf-ID provided in the INVITE message from the Downstream conference aware UA by sending a SUBSCRIBE message to the Downstream conference aware UA. (Optional)
49. The Downstream conference aware UA acknowledges the subscription request by sending a 200 OK message back to the caller. (Optional)
50. The Downstream conference aware UA then returns a NOTIFY message to the caller to provide subscription status information. (Optional)
51. The Downstream/transfer-to PSAP responds by returning a 200 OK message. (Optional)

At this point, the Upstream/transfer-from PSAP has dropped and the caller and the Downstream/transfer-to PSAP are communicating via the Downstream conference aware UA.

The Downstream/transfer-to PSAP can terminate the call using the sequence in Section 4.7.1.3.4. If the Upstream ESInet (with Route All Calls Via a Conference Aware UA) employed a B2BUA, the B2BUA would replace the caller in the above sequence. Note as before if the B2BUA anchored media, a possible tromboning of the media path could occur.

Note that if, at some point, the transfer-from PSAP adds another transfer-to PSAP in the same Downstream ESInet to the call prior to the transfer-from PSAP dropping out of the call, it would transit the Downstream conference aware UA, and the Downstream conference aware UA would act as a B2BUA to that leg also (not illustrated).

© Copyright 2011-2022 National Emergency Number Association, Inc.

4.10 Location Information Server (LIS)

A Location Information Server supplies location in the form of a PIDF-LO (location by value) or a location URI (location by reference). The LIS also provides a "dereference" service for a location URI it supplies: given the URI, the LIS provides the location value as a PIDF-LO. A LIS MAY be a database, or MAY be a protocol interworking function to an access network-specific protocol.

In NG9-1-1, the LIS supplies location (by value or reference) to the endpoint, or to a proxy operating on behalf of the endpoint. The ESInet is not directly involved in that transaction: the resulting PIDF-LO or location URI must appear in the initial SIP message in a Geolocation header field. If the LIS supplies location by reference, it MUST also provide dereferencing service for that location URI. Elements in the ESInet, including the ESRP, and the PSAP may dereference a location URI as part of processing a call.

If the LIS supplies location by reference, it MUST support HELD (RFC 5985) [7], HELD Dereferencing (RFC 6753) [55], and/or SIP Presence Event Package (RFC 3856) [25]. The SIP Presence SUBSCRIBE/NOTIFY mechanism can control repeated dereferencing, especially when tracking of the caller is needed. However, HELD is acceptable on any location URI. LISs supporting SIP MUST support location filters (RFC 6447) [72] and event rate control (RFC 6446) [80].

If the broadband access network supports true mobility, it SHOULD supply location by reference. If the broadband network is a fixed network like a cable modem network or DSL, location by value is preferred, but location by reference is acceptable.

The LIS MAY support SIP Presence to provide location-by-reference as defined by RFC 5808 [54]. Using SIP Presence, the entity desiring location subscribes to the SIP Presence Event Package (RFC 3856 [25]) at the location URI provided[45]. The LIS sends NOTIFY transactions (RFC 6665 [14]) containing a PIDF document that will include the location in the Location Object (LO) part, forming the PIDF-LO. An immediate NOTIFY will be generated by the LIS upon acceptance of a subscription request. This would represent the current location of the target. The SUBSCRIBE includes an Expires header field (RFC 3261) [10] which represents the subscribers requested expiration, and the 2XX response contains one that represents the server's actual expiration (which may be shorter, but not longer, than the subscriber's requested time). An Expires of zero indicates a request for exactly

[45] The entity providing a SIP Presence-based location URI should always provide a sips: URI and not a sip: URI, although calls must not fail if credentials are not available. pres: URIs must never be used for this application.

© Copyright 2011-2022 National Emergency Number Association, Inc.

one NOTIFY (that is the current location) with no further updates. Subscriptions expire when the call terminates if the LIS is call-aware.

The querier can limit how often further NOTIFYs are sent (before expiration of the subscription) using a filter (RFC 4661 [92]). Rate limits (RFC 6446 [80]) and Location filters (RFC 6447 [72]) are useful for this application and must be supported by the LIS if it supplies a SIP location URI[46].

A LIS MUST validate locations prior to entering them into the LIS using the LVF (see Section 4.3).

A LIS MAY support the validation of location around planned changes as defined by draft-ecrit-lost-planned-changes [178].

A LIS MUST accept credentials traceable to the PCA for authenticating queries for a location dereference. Since calls may be diverted to any available PSAP, the LIS cannot rely on any other credential source to authorize location dereferencing.

When location is provided by reference there is a need for the reference to be valid at least for the length of the call. Since the call may be transferred to a transfer-to PSAP for handling, the transfer-to PSAP must have the ability to dereference the location reference provided with the call. It is therefore critical that the location URI not expire before the transfer-to PSAP has the opportunity to dereference it. RFC 6753 [55] suggests that there SHOULD be an expiration time associated with location URIs, and RFC 5985 [7] provides that it SHOULD be set at a minimum of 30 minutes, with a maximum of 24 hours. To be consistent with these recommendations, any LIS that provides a dereferencing service for a location URI MUST provide an expiration time associated with that URI set at a minimum of 30 minutes, with a maximum of 24 hours.

Providing location beyond the length of the call raises privacy concerns. Sometimes, users can control access to their location by means of a privacy policy that they can specify. During an emergency call, there is no universal expectation of privacy of location. When the call completes, privacy should be restored. Some LISes do not have an explicit privacy policy but consider access to user's location on a case-by-case basis, often with commercial implications.

While there are some circumstances in which it is desirable that location be made available to 9-1-1 after a call completes, it cannot be required without a change in law. Therefore, it

[46] If an entity receives a SIP URI for location by reference and specifies an expiration time greater than zero, it will usually get more than one NOTIFY. If it specifies a filter, then the filter determines when and how often the NOTIFYs are generated. If no filter is specified, the entity will determine how often to send NOTIFYs using an algorithm of its choice.

© Copyright 2011-2022 National Emergency Number Association, Inc.

is not required that a LIS honor any request from NG9-1-1 entities following completion of a call. LIS operators who do not give their users control of privacy should consider balancing privacy needs with the occasional requirement of NG9-1-1 entities to get a location update. The NG9-1-1 authentication processes provide mechanisms to determine the role of the agent making a request, and restricting access after a call to supervisory personnel could be considered. NG9-1-1 entities cannot assume location will be available after a call.

4.11 Additional Data Repository (ADR)

An Additional Data Repository is a source of Additional Data. URIs pointing to the ADR may be passed in a call, in an EIDO, or by other mechanisms. Each URI could point to a different ADR. In response to an HTTPS GET of the URI, the ADR returns the referenced Additional Data block.

An emergency call MUST have at least two[47] Call-Info header fields, each with a URI that resolves to an Additional Data structure (RFC 7852) [107] (the required block types are EmergencyCallData.ProviderInfo and EmergencyCallData.ServiceInfo). Each URI may be a Content Identifier (CID) that references an Additional Data block in the in the body of an INVITE or MESSAGE, or an HTTPS URI to an external source. Additionally, the <provided-by> element of a PIDF-LO may contain an Additional Data URI or an Additional Data block. The external database that dereferences external Additional Data URIs is an Additional Data Repository (ADR). There is a minimum amount of information listed as Mandatory for EmergencyCallData.ProviderInfo and EmergencyCallData.ServiceInfo that, when combined with information from the PIDF-LO and the SIP INVITE or MESSAGE, is minimally equivalent to the information currently provided by all originating networks in the ALI.

All originating networks and service providers[48] are expected to provide at least this minimum set of information either by reference or value. Access networks are expected to provide the same minimum set of information. Each Call-Info header field with a purpose parameter value starting with "EmergencyCallData", a dot, and a block name references an Additional Data block (either by value or by reference). It is important that ALL originating networks and service providers handling the call add Call-Info header fields when they can be reasonably expected to determine they are handling an emergency call. It is also important that ALL entities that provide a PIDF-LO when they can be reasonably expected

[47] Wireline and other legacy networks that historically provide subscriber information are expected to continue to do so using the SubscriberInfo block of Additional Data.

[48] In the context of Additional Data, the term "service provider" refers to a 3rd party, in the path of an emergency call or not, and which is not the originating network presenting the call to the ESInet.

© Copyright 2011-2022 National Emergency Number Association, Inc.

to determine it is for an emergency call include a <provided-by> element in the PIDF-LO to indicate the source of the PIDF-LO. The transaction to dereference the Additional Data URI MUST be protected with TLS. The dereferencing entity, which may be an ESRP, LPG, PSAP, or responding agency, uses its credentials (traceable to the PCA for NG9-1-1 entities) to dereference the Additional Data URI. The originating network or service provider can use any credential, as long as the domain listed in the URI is the domain of the SubjectAltName in the credential.

ADRs can host sensitive data for which the disclosure may be subject to legal, regulatory, privacy and confidentiality requirements, and/or local policy. Such requirements may supersede the stated requirements herein. All ADR queries originating within an ESInet MUST include authentication by credentials traceable to the PCA. An ADR MAY serve less-sensitive data in the event PCA-traceable authentication fails. All ADRs MUST serve data for any valid query. A call-stateful ADR MAY limit the length of time that it will serve data after the end of the associated emergency call. Such a time limit SHOULD be at least five minutes. ADRs may not have the data themselves, but may know where the data can be found. The response to a dereference request can be redirected to another ADR with an HTTPS 333 response (Iterative Refer).

Devices such as those within telematics-equipped vehicles and medical monitoring devices that can place emergency calls may provide Additional Data blocks by value or by reference within the INVITE or MESSAGE. When provided by reference, devices could have the capability to respond to an ADR query themselves or could publish data to an external ADR. A service provider (such as a telematics service provider) could provide the ADR instead of the device. Other devices could also provide an ADR for use in an emergency call. There may be multiple Additional Data blocks, each of which may be provided by reference or by value by the device, originating network, or service provider. (See Section 3.1.19 for more information about telematics calls and datasets.)

Additional Data blocks may be provided by reference or by value by the access network, originating network, or service provider. When service providers, access and originating networks only provide the minimal data called for in RFC 7852 [107], the ADR could be provided by a third party. For Additional Data provided by the calling entity itself, the data could be conveyed by value within the INVITE or MESSAGE, or by reference via an ADR that could be provided by the calling entity or a third party.

Interaction with the ADR MUST be protected by TLS. The ADR MUST accept certificates traceable to the PCA. ESInet entities may only accept certificates for the ADR signed by a CA recognized by common web browsers.

A class of ADRs provides an additional capability to be searched by an identity. See Section 4.11.1 for specifications for this capability.

© Copyright 2011-2022 National Emergency Number Association, Inc.

4.11.1 Identity Searchable Additional Data Repository (IS-ADR)

Some Additional Data Repositories have an optional feature that allows the repository to be searched by identity. This capability is needed when data is stored by an entity that is not in the path of the call or access network. For example, personal medical data provided by the caller may be stored by an entity trusted by the caller to keep such data. The caller provides the identity it uses on calls, and the IS-ADR is searched. An IS-ADR is an ADR and MUST conform to Section 4.11.

The IS-ADR provides a web service. When queried with a caller's From address or P-Asserted-Identity (as retrieved from the SIP header field)[49], the IS-ADR returns one of the following in response:

- The caller's Additional Data (by value);
- A URI that can be used to dereference the caller's Additional Data;
- An HTTP 307 Temporary Redirect instructing the client to direct an Additional Data query to the resource specified in the response;
- An indication that no data was found for the provided From or P-A-I URI.

The OpenAPI definition of this web service may be found in Appendix E.2.

IdentitySearchRequest

HTTP method: GET

Resource name .../AdditionalData

Request Parameters:

Name	Condition	Description
CallerURI	MANDATORY	URI of caller From/P-A-I

A successful query returns an Additional Data Value in a string

Status Codes

200	OK
307	Temporary Redirect
404	Not Found
454	Unspecified Error

[49] The "From" SIP header field may be used if the P-Asserted-Identity field (P-A-I) is not present, as P-A-I may not be retained on SIP calls which cross untrusted domains.

© Copyright 2011-2022 National Emergency Number Association, Inc.

It is anticipated that a number of third parties will choose to host an IS-ADR. A registry of recognized IS-ADRs is defined. PSAPs and other responsible parties can then use the IANA IS-ADR registry as input into the configuration of the NG9-1-1 functional elements under their control.

Note: A privacy issue was identified associated with this mechanism. Since it will require substantive changes, this will be addressed in a future version of this document.

4.12 Logging Service

The Logging Service in NG9-1-1 is a standardized functional element used by all elements in an ESInet to log all significant events; logging is not restricted to events within a PSAP. All significant steps in processing a call are logged. NG9-1-1 defines an external Logging Service interface so that the logging function can be provided in the ESInet (i.e., external to a PSAP). Logging includes external events, internal events, media, and messages. All forms of media described in this document MUST be logged (see the Media section for details). Media recording SHOULD begin at the earliest point possible, which can be before the call has been answered if early media are available; recording media both at or near ESInet ingress and within a PSAP is desirable. The Logging Service is sometimes referred to as simply "the Logging Service" in this document. Each agency can have its own Logging Service, or Logging Services can be shared. Since incidents may involve multiple agencies, obtaining logging records from multiple Logging Services may be required. The Agency Locator record includes the URI to the Logging Service for a particular agency.

The Versions entry point of the Logging Web Service MUST include, in the "serviceInfo" parameter, the parameter "requiredAlgorithms" whose value is an array of JWS algorithms (as described in 5.10) acceptable to the Logging Service. The following example is from a Logging Service whose currently in force policy permits unsigned LogEvents as well as signed LogEvents using the "EdDSA" algorithm:

```
{
  "fingerprint": "Woof-FurrySuite-v8-8c439e",
  "versions":
          [
       { "major": 6, "minor": 3,
         "vendor": "burby-magic",
         "serviceInfo": { "requiredAlgorithms": [ "EdDSA", "none" ] }
       }
    ]
}
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

4.12.1 Logging Introduction

The Logging Service incorporates a web service that supports logging and retrieving events. In addition to the web service interface, Logging Services MUST implement a Session Recording Protocol (SIPREC - RFC 7866) interface [116] for recording the media and, if provided, the associated metadata. Logging Services MUST provide a Real-time Streaming Protocol (RTSP) interface compliant with RTSP 2.0 (RFC 7826 [98]) to play back the media. RTSP 1.0 MUST NOT be used. The web service includes the functions described in the LogEvent section.

Clients to the Logging Service MUST support logging to at least two Logging Services for redundancy purposes, with support for three (3) or more RECOMMENDED, and some jurisdictions might require four or more. The Logging Service is NOT intended to support other kinds of devices that may wish to operate from the LogEvent records. See LogEventReplicator, Section 4.12.3.9.

Each Logging Service FE MUST implement the server-side of the ElementState event notification package. The Logging Service FE MUST promptly report changes in its state to its subscribed elements.

The set of Logging Service FEs within an NGCS MUST implement the server-side of the ServiceState event notification package for the Logging Service. ESInets can be built with Logging Services either local or centralized, and less commonly a mix of both local and state level Logging Services. Accordingly, it is recommended that each NGCS that provides a Logging service implement ServiceState for that NGCS.

4.12.2 Media Recording Interface

The Logging Service acts as a Session Recording Server (SRS) and accepts media and metadata from a Session Recording Client (SRC) as defined in the Session Recording Protocol (RFC 7866) [116]. The Logging Service MUST implement the SRS interface. Any element that has RTP-transported call media MAY deploy the SRC interface and at least one element in the call path MUST deploy the SRC interface. All Bridge elements (Section 5.7), Gateway elements (Section 7), BCF elements that anchor media, and PSAP Call Handling elements, MUST implement the SRC interface. Overall ESInet design determines which elements may be provisioned to record. Such designs MUST assure that media are always recorded, even when calls are handled out-of-area, which may make different assumptions than the local ESInet on such matters. Elements that implement the SRC interface MUST be capable of supporting redundant implementations of the SRS (RFC 7866) [116] and MUST insert the Call Identifier and Incident Tracking Identifier (Call-Info header fields) defined in this document into the INVITE sent to the Logging Service.

© Copyright 2011-2022 National Emergency Number Association, Inc.

The logging recorder that supports the Session Recording Server (SRS) functionality defined in the SIPREC specification (RFC 7866) [116] interfaces to any Functional Elements that support a Session Recording Client (SRC).

The Logging Service and its SRC interface MUST log the SIPREC Metadata LogEvent (see the LogEvent section for details). An SRC MAY support sending SIPREC Metadata (RFC 7865) [117]. When an SRC sends SIPREC Metadata, it MUST generate a SiprecMetadata LogEvent to the Logging Service. The SRC MUST include the CallId and IncidentId for the emergency call being recorded in the SIPREC INVITE it generates and when generating an associated SiprecMetadata LogEvent.

Each emergency call (that is, each Communication Session), MUST result in a separate Recording Session. More than one Recording Session MAY be logged for a single call.

All SRCs and SRSes MUST implement RTCP on the recording session. The SRC MUST send wall clock time in sender reports, which MUST be recorded by the SRS. This allows media synchronization of multiple media streams on playback.

SRCs MUST support recording of media to at least two SRSes.

The flow diagrams are informative and do not attempt to show every case.

The following events have been omitted for clarity:

- The OK on the BYE
- Provisional messages
- ACKs

In the below example, "Answering Point" is an element inside a PSAP and may not have a standardized interface. "Ring", "Answer", and "Dial" are used as the names of the messages, as the Answering Point protocol is out of scope.

RS = Recording Session as defined in SIPREC.

CS= Communication Session as defined in SIPREC.

The call MUST go on even if there is no recorder.

4.12.2.1 Incoming Call

The SRC opens a recording session with the logging recorder. The call between the Caller and Answer-Point is recorded for its duration. The call flow for this scenario is:

- Call hits the SRC
- SRC opens a recording session with the recorder, including the call identifier
- Call is answered
- Call stream is added to the recording session

© Copyright 2011-2022 National Emergency Number Association, Inc.

- Both parties communicate
- Caller hangs up
- Answer-Point hangs up
- SRC closes the recording session.

Note: All additional information about the call can be retrieved from the Logging Service using the call identifier.

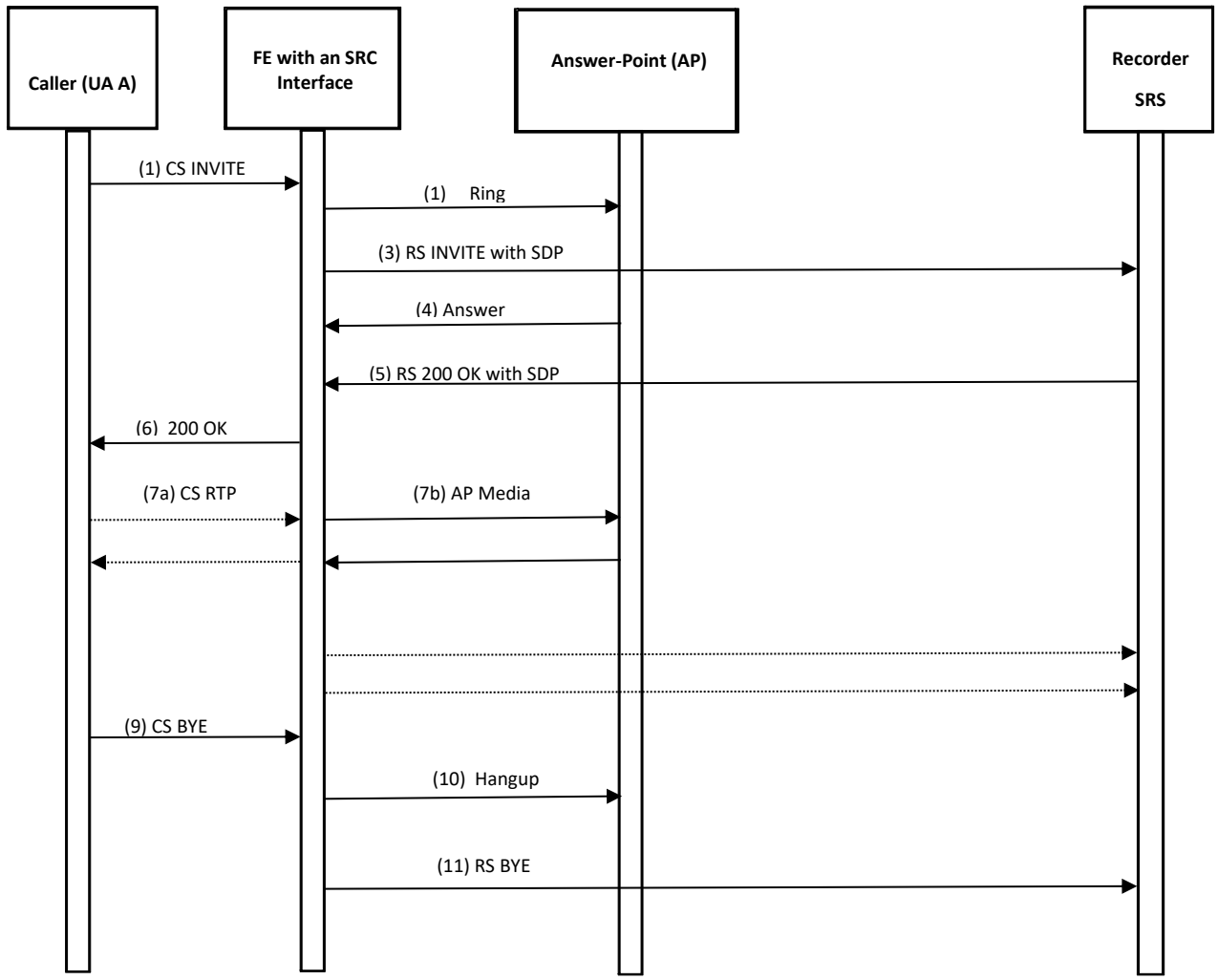


Figure 4-15 Incoming Call

© Copyright 2011-2022 National Emergency Number Association, Inc.

4.12.2.2 Three Party Call (e.g. translator)

The Answer-Point establishes a two-party call and conferences in a third party. The call MUST still be recorded while the third party is being added as well as when all three parties are on the call.

- Call hits the SRC
- SRC opens a recording session with the recorder, including the call identifier
- Call is answered
- Call stream is added to the recording session
- Both parties communicate
- Answer-Point calls 3rd Party
- Call is answered by 3rd Party
- Re-invite is sent to the recorder with the call identifier 3rd Party stream is added to the recording session
- All parties communicate
- Caller hangs up
- 3rd Party hangs up
- Answer-Point hangs up
- SRC closes the recording session.

Note: All additional information about the call can be retrieved from the Logging Service using the call identifier.

© Copyright 2011-2022 National Emergency Number Association, Inc.

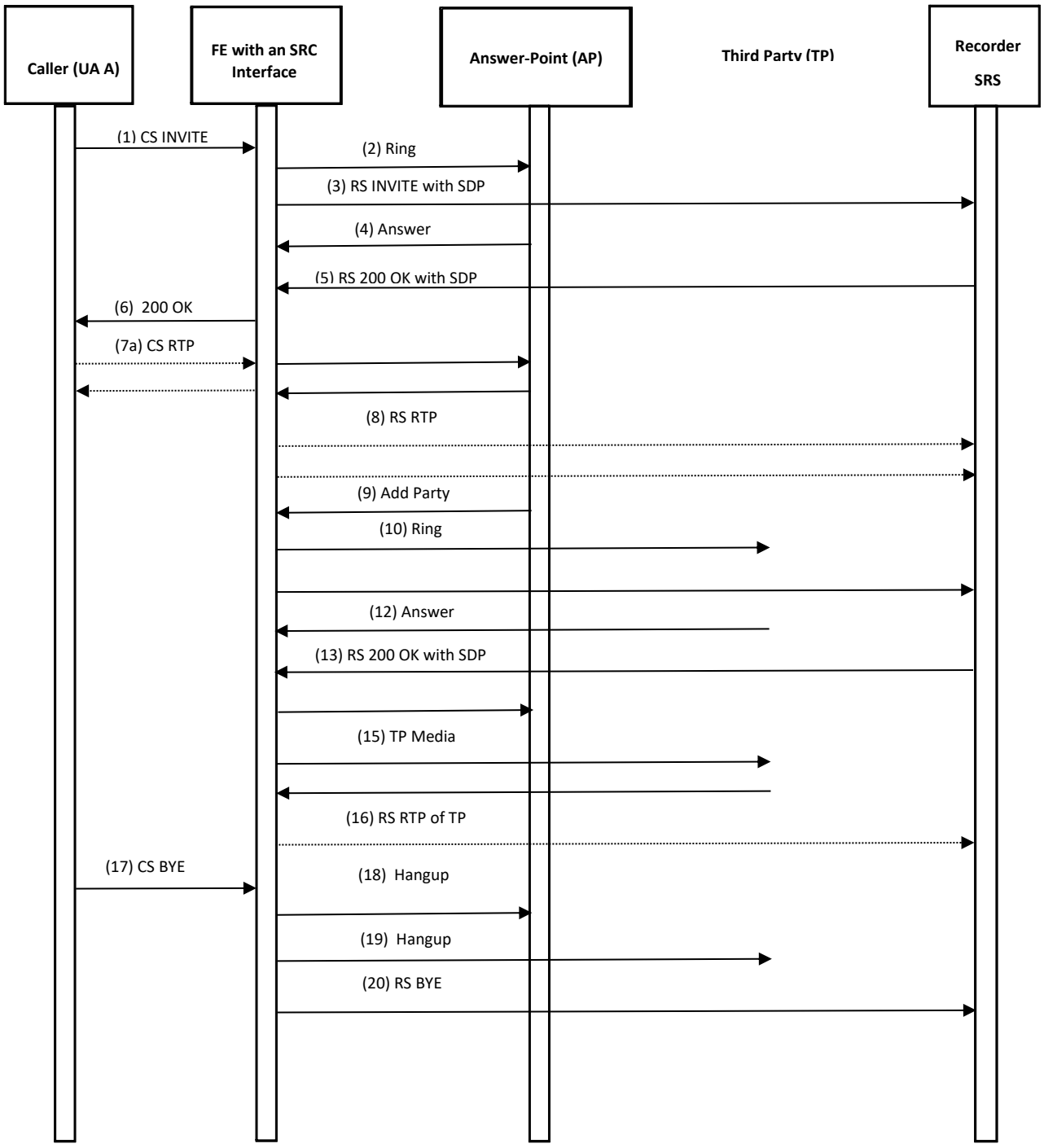


Figure 4-16 Three-Party Call

© Copyright 2011-2022 National Emergency Number Association, Inc.

4.12.2.3 Attended Transfer

The Answer-Point transfers the call to a third party. The call MUST still be recorded if it is bridged by the SRC.

- Call hits the SRC
- SRC opens a recording session with the recorder, including the call identifier
- Call is answered
- Call stream is added to the recording session
- Both parties communicate
- Answer-Point calls 3rd Party
- Call is answered by 3rd Party
- Re-invite is sent to the recorder with the call identifier
- 3rd Party stream is added to the recording session
- Answer-Point hangs up
- Remaining parties continue to communicate
- Caller hangs up
- 3rd Party hangs up
- SRC closes the recording session.

Note: All additional information about the call can be retrieved from the Logging Service using the call identifier.

© Copyright 2011-2022 National Emergency Number Association, Inc.

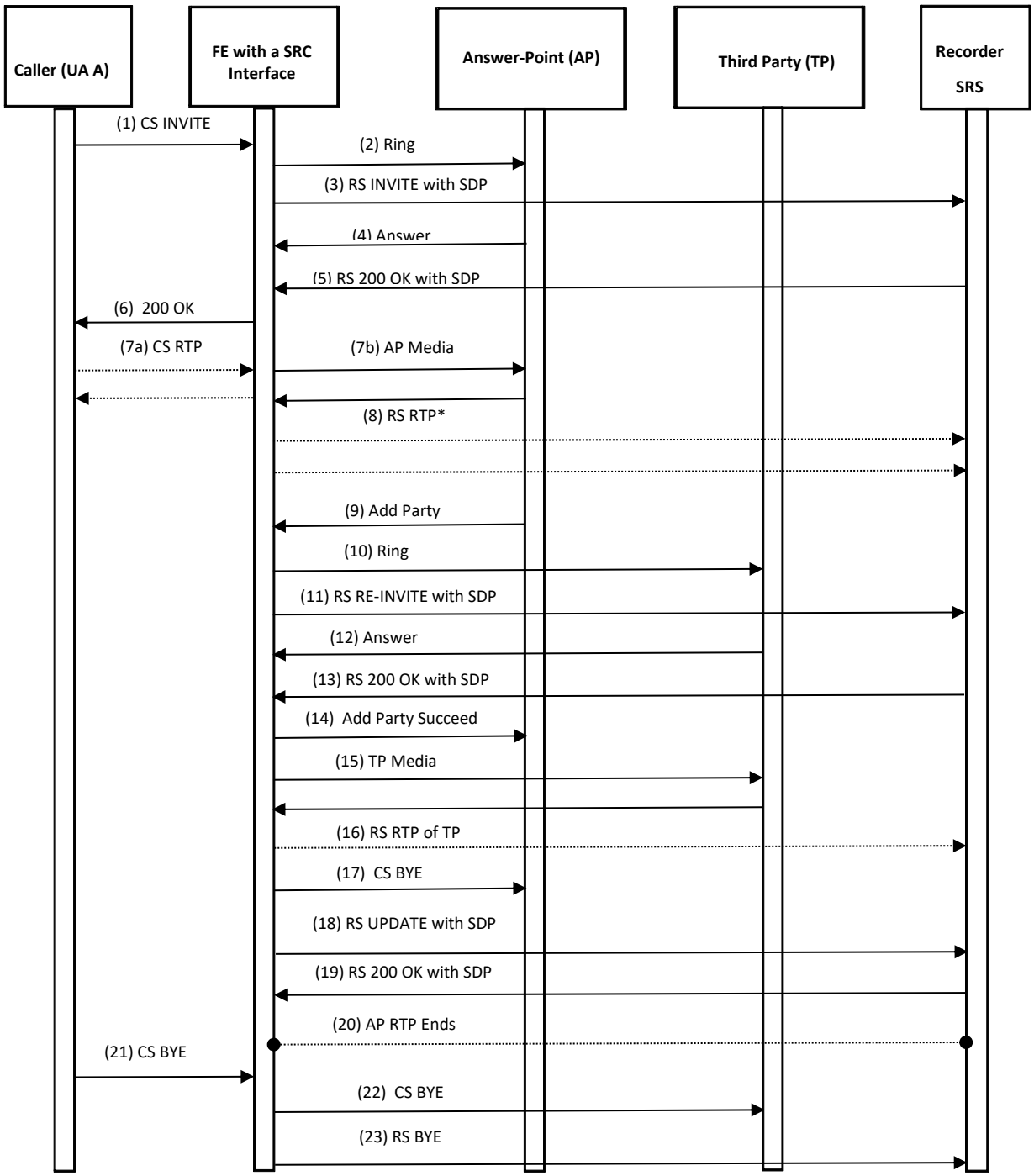


Figure 4-17 Attended Transfer

* RTP stream from Answer-Point to Recording Server in Step 8 stops.

© Copyright 2011-2022 National Emergency Number Association, Inc.

4.12.2.4 Call Back (Outbound Call)

The SRC initiates an outbound call via recorded administrative line in response to a 9-1-1 hang-up or dropped call. The call between the Originating-Point and the Caller is recorded for its duration. The call flow for this scenario is:

- Call is initiated in response to 9-1-1 call that was disconnected due to hang-up or drop
- SRC opens a recording session with the recorder, including the call identifier
- Call is answered by the previously disconnected caller
- Call stream is added to the recording session
- Both parties communicate
- Called party hangs up
- SRC Originating Point hangs up
- SRC closes the recording session.

Note: All additional information about the call can be retrieved from the Logging Service using the call identifier.

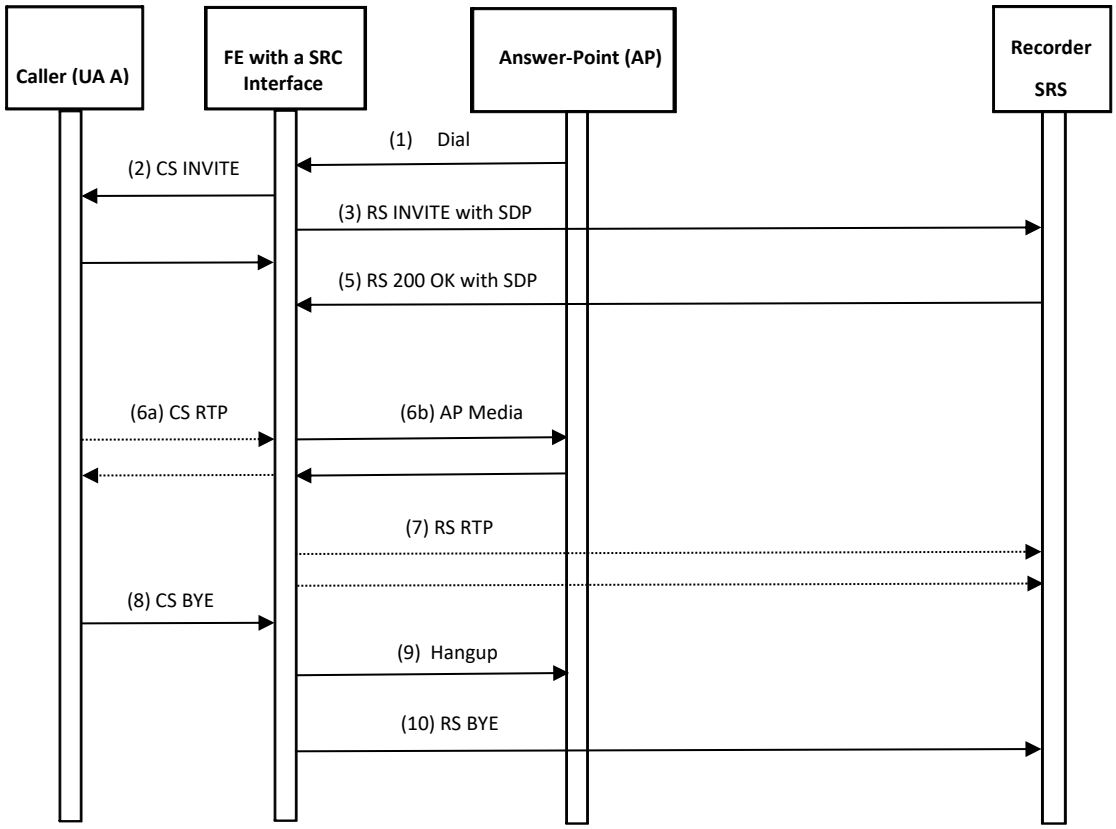


Figure 4-18 Call-Back

© Copyright 2011-2022 National Emergency Number Association, Inc.

4.12.2.5 Blind Transfer

The Answer-Point transfers the call to a third party as an unsupervised transfer. The call MUST still be recorded by the SRC.

- Call hits the SRC
- SRC opens a recording session with the recorder, including the call identifier
- Call is answered
- Call stream is added to the recording session
- Both parties communicate
- Answer-Point calls 3rd Party
- Answer-Point hangs up
- Re-invite is sent to the recorder with the call identifier
- 3rd Party stream is added to the recording session
- All parties communicate if and when 3rd party answers
- Caller hangs up
- 3rd Party hangs up
- SRC closes the recording session.

Note: All additional information about the call can be retrieved from the Logging Service using the call identifier.

© Copyright 2011-2022 National Emergency Number Association, Inc.

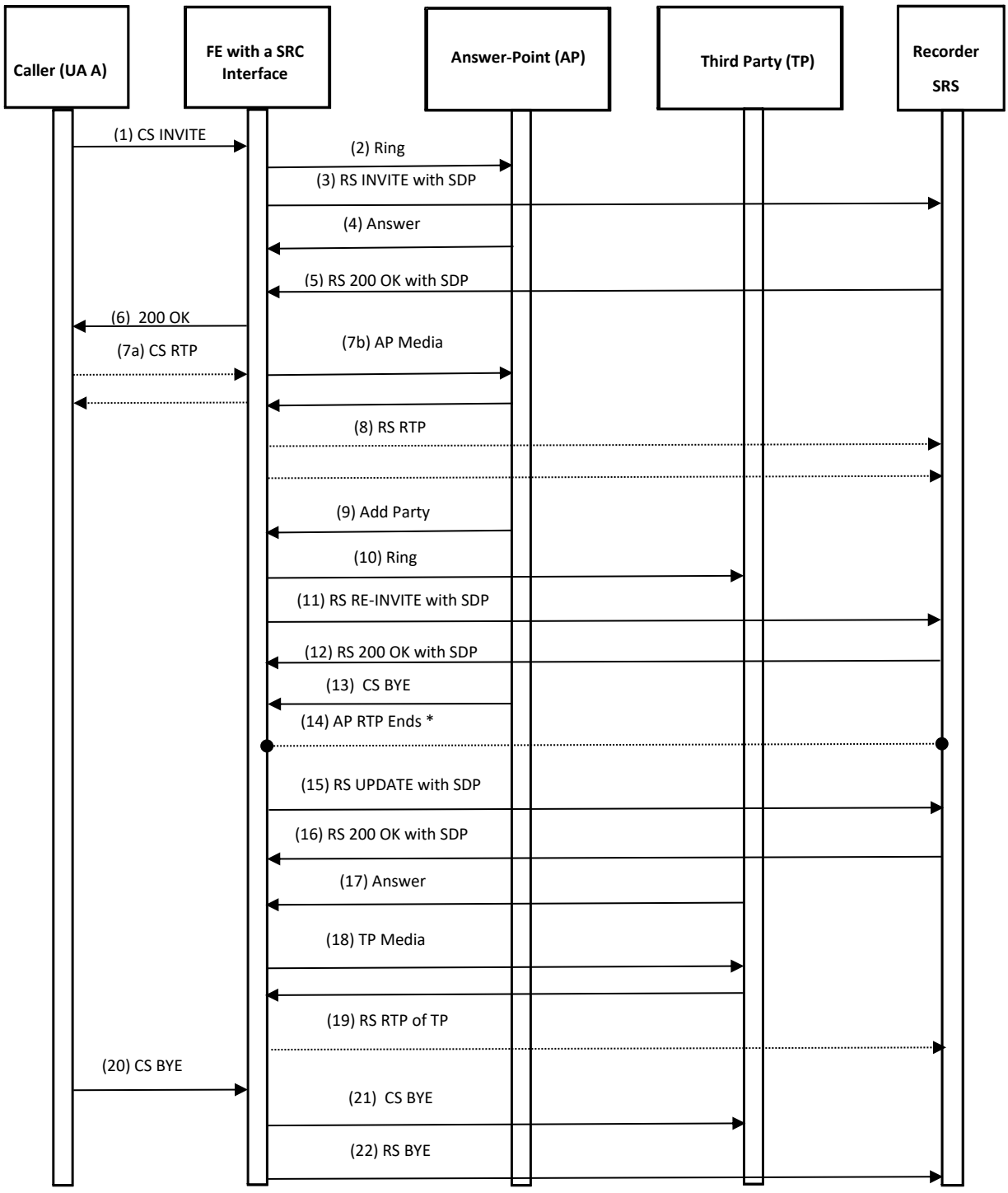


Figure 4-19 Blind Transfer

© Copyright 2011-2022 National Emergency Number Association, Inc.

4.12.2.6 Clean Logging Service Shutdown

The Logging Recorder MUST be able to provide a clean shut down by sending a BYE as specified in Section 3.1.1.3, for example when one SRS in a redundant pair is going out of service. The SRC MUST respond with a 200 OK.

- Call hits the SRC
- SRC opens a recording session with the recorder, including the call identifier
- Call is answered
- Answer-Point stream is added to the recording session
- Both parties communicate
- Recorder sends a BYE
- SRC responds with a 200 OK.

Note: All additional information about the call can be retrieved from the Logging Service using the call identifier.

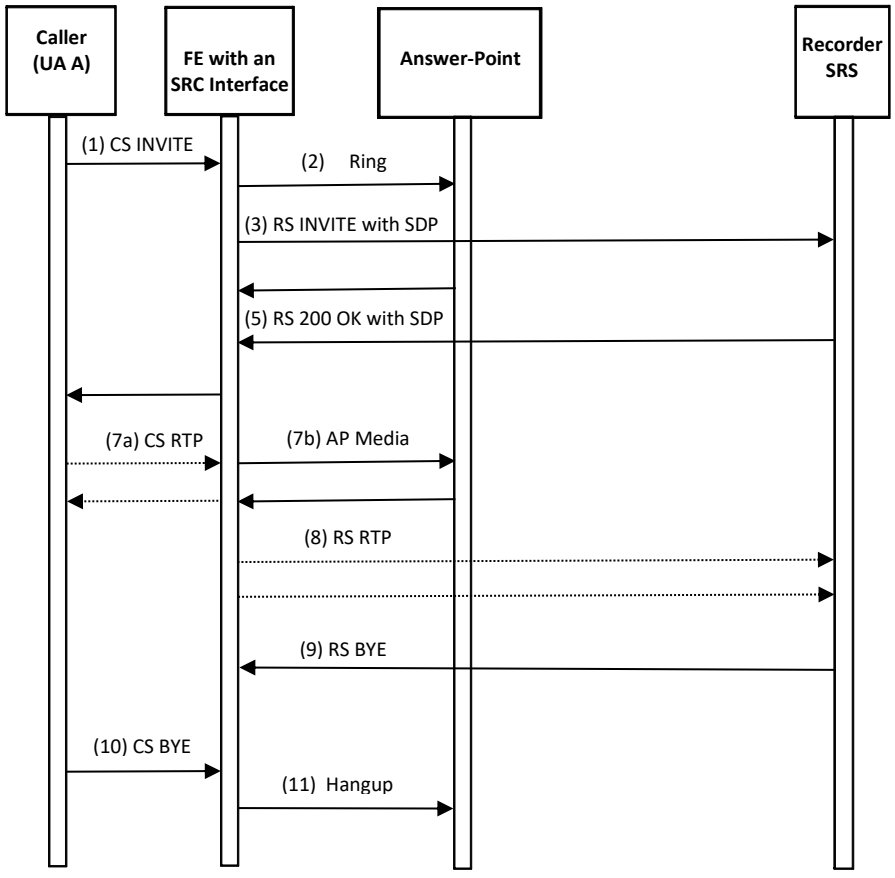


Figure 4-20 Logging Service Shutdown

© Copyright 2011-2022 National Emergency Number Association, Inc.

4.12.3 Log Recording

The OpenAPI definition of this web service may be found in Appendix E.8. The Logging Service has a policy (LogServiceAllowedToLog) of which entities are permitted to LogEvents, and a policy (LogServiceAllowedToRetrieve) of which entities are allowed to retrieve logged events.

Note: A future edition of this document will describe how policies can restrict retrieval by more fine-grained criteria, for example allowing only agencies participating in a multi-agency incident to retrieve LogEvents about that incident.

Entities might periodically review signed events to verify that their signatures are correct and they have an accessible and valid certificate (and thumbprint for certificates provided by reference). An entity that does so generates a Log Signature/Certificate Discrepancy Report (Section 3.7.22) to report problems to the logging entity. (As examples, a Logging Service might perform this process when it is under light load, or another entity might be configured to do this at certain intervals.)

4.12.3.1 LogEvents

The Logging Service stores LogEvents as a JWS. A LogEvent object contains:

Name	Condition	Description
clientAssignedIdentifier	OPTIONAL	An identifier assigned by the client
logEventType	MANDATORY	LogEvent type as described in Section 4.12.3.7
timestamp	MANDATORY	A Timestamp as defined in Section 2.3
elementId	MANDATORY	Element identifier (Section 2.1.3) of the element that logged the event
agencyId	MANDATORY	AgencyId (Section 2.1.1) of the agency that logged the event
agencyAgentId	Conditional: REQUIRED if the log record is traceable to an agent. If the log record is only attributable to an element or agency, this element will not be included.	The Agent Identifier (Section 2.1.2) of an agent that logged the event.

© Copyright 2011-2022 National Emergency Number Association, Inc.

Name	Condition	Description
agencyPositionId	OPTIONAL	Identifier for the position that is handling a call.
callId	Conditional: REQUIRED if event is associated with a call	The Call Identifier of a call, see Section 2.1.6
incidentId	Conditional: REQUIRED if event is associated with an Incident	The Incident Tracking Identifier associated with the call, see Section 2.1.7
callIdSIP	Conditional: REQUIRED if event is associated with a SIP call	CallId from SIP
ipAddressPort	Conditional: REQUIRED if logging element knows the identity of the other element	Normalized IP address and port number string or Fully Qualified Domain Name of another element that participated in a transaction that triggered this LogEvent (e.g., an element that sent or responded to a query). This is not the address of the element that logs the event. For IPv6 addresses, the maximum uncompressed form is recommended and may be required in a future version of this document. (See *A Recommendation for Ipv6 Address Text Representation*, RFC 5952 [196].
extension	OPTIONAL, occurs 0 or more times	Optional private extension parameters

The Logging Service stores and retrieves a JWS [171] of the entire LogEvent (see Section 5.10), including all extensions. The signer (using its credentials traceable to the PCA) is: the Agent if an agencyAgentId is provided, otherwise it is the Element.

The signature is optional, but policy of the agency may require its use.

The clientAssignedIdentifier is not used by the Logging Service but is preserved by it.

© Copyright 2011-2022 National Emergency Number Association, Inc.

The callId and incidentId are provided on all legs of a dialog-forming SIP transaction initial message (INVITE or MESSAGE). Stateless proxies may not know the IDs and thus may not be able to provide them, and some implementations may not be able to provide the IDs on other messages in the transaction. The Logging Service will need to find such messages via callIdSIP.

This document specifies very detailed logging, often requiring an event to be logged by both the sender and receiver of data. This detail is invaluable for troubleshooting errors in processing after the fact. The amount of data being logged is typically a small fraction of the size of the media for the same call.

The LogEvent object contains an "extension" member which is used to log any desired proprietary data in a Logging Service. The size of any object, with all its extensions, may be limited to a provisionable value by the Logging Service, and the operator of a Logging Service may have an approved list or disallowed list of allowed extensions.

Logging services MUST NOT require any specific extension to provide services conformant to this document. FEs that use a Logging Service MUST NOT depend on a Logging Service accepting an extension to provide services conformant to this document. Each EventType contains additional data specific to the EventType.

The parameters are sent as a JWS [171] (see Section 5.10).

As described in Section 5.10, the Logging Service MUST be capable of handling signed and unsigned LogEvents and certain signing algorithms. The policy currently in force at the Logging Service determines the Logging Service's acceptance of signed and unsigned LogEvents, which could require only signed LogEvents, only unsigned LogEvents, or could allow either. This policy is communicated to logging clients by the "requiredAlgorithms" parameter, which as described above (Section 4.12) specifies the currently acceptable signing algorithms. If "requiredAlgorithms" contains only the value "none", then only unsigned LogEvents are acceptable; if "requiredAlgorithms" does not contain the value "none", unsigned LogEvents are not acceptable. A LogEvent request containing a LogEvent whose JWS "alg" element value is not contained in "requiredAlgorithms" is rejected with an "Unacceptable Algorithm" error. This is an error response; the LogEvent is not recorded (although the Logging Service might log or record that it received such a request with details); the client needs to resubmit the request with an acceptable algorithm.

Logging Services MUST be capable of verifying the signature of a signed LogEvent during the processing of the LogEvent request (i.e., before returning the response). The currently in force policy of the agency operating the Logging Service determines if the Logging Service does so. If the signature verification fails, it MUST return a "Signature Verification Failed" status code as a warning and SHOULD generate (subject to throttling) a

© Copyright 2011-2022 National Emergency Number Association, Inc.

Signature/Certificate Discrepancy Report (Section 3.7.22) to the logging entity. This is a warning, not an error; the LogEvent MUST be recorded, and the client MUST NOT retry the request. An entity receiving this warning should generate an internal DR or otherwise alert its operational staff to the problem and might choose to fall back to a previous certificate until the problem is corrected.

Verifying LogEvent signatures requires access to the certificate used to sign the event (and all intermediate certificates to a trusted root). The entity creating a signed LogEvent specifies the certificate either by value or by reference, as described in Section 5.10. A Logging Service MUST support both mechanisms (e.g., by using a certificate cache indexable by thumbprint and loaded by resolving the certificate URL).

The CallId and IncidentId are provided on all legs of a dialog-forming SIP transaction initial message (INVITE or MESSAGE). Stateless proxies may not know the IDs and thus may not be able to provide them, and some implementations may not be able to provide the IDs on other messages in the transaction. The Logging Service will need to track such messages (via the SIP call identifier) and log the Call and Incident IDs.

This document specifies very detailed logging, often requiring an event to be logged by both the sender and receiver of data. This detail is invaluable for troubleshooting errors in processing after the fact. The amount of data being logged is typically a small fraction of the size of the media for the same call.

To allow including proprietary data in LogEvents, the LogEvent object MAY contain additional elements not defined in this document. The size of any object, with all its extensions, may be limited to a provisionable value by the Logging Service, and the operator of a Logging Service may have an approved or disallowed list of allowed extension elements.

Logging services MUST NOT require any specific extension to provide services conformant to this document. FEs that use a Logging Service MUST NOT depend on a Logging Service accepting an extension to provide services conformant to this document. Each LogEventType contains additional data specific to the LogEventType.

4.12.3.1.1 Retrieve LogEvents

Retrieves LogEvents from the Logging Service. For a GET operation the response is the log record for all events. Limit and start parameters are supported for pagination.

HTTP method: GET

Resource name .../LogEvents

When the event is a RecMediaStartEvent, the returned events will have one or more "rtsp" parameters inserted by the Logging Service that MUST be RTSP URIs. The RTSP URI can

© Copyright 2011-2022 National Emergency Number Association, Inc.

be used to play back the call session. The "sdp" and "mediaLabel" are also returned to indicate which media stream in the session the event refers to. These "rtsp" parameters MUST NOT refer to media from other SIPREC sessions that recorded the same call. Because the IRR functionality uses this interface, the Logging Service MUST ensure that it can return a usable RTSP URL as soon as recording starts. The Logging Service MUST ensure that any RTSP URL it returns remains valid for at least one hour.

The Retrieve Events includes the following parameters:

Name	Condition	Description
limit	OPTIONAL	Maximum number of results to return
start	OPTIONAL	First item in the page of results, as an ordinal 1-based integer.
logEventType	OPTIONAL	Type of LogEvent, if not provided, events of any type are returned
startTime	OPTIONAL	If provided, only events timestamped at or after this time will be returned
endTime	OPTIONAL	If provided, only events timestamped at or before this time will be returned

Status Codes

200 LogEvents found
404 Not Found

On a successful GET, a logEventContainerArray is returned:

logEventArray

Name	Condition	Description
count	MANDATORY	Number of items in the array
totalCount	MANDATORY	Total number of items found
logEventContainers	MANDATORY	Array of LogEventContainer objects

A LogEventContainer contains:

© Copyright 2011-2022 National Emergency Number Association, Inc.

logEventId	MANDATORY	LogEvent Identifier assigned by the logging service as described in Section 2.1.8
rtsp	CONDITIONAL	rtsp parameters returned from RecMediaStartEvent. MUST be returned if media was recorded
logEvent	MANDATORY	A LogEvent in JWS format

4.12.3.1.2 Post Event

Logs a new event into the Logging Service.

HTTP method: POST

Resource name .../LogEvent

The body of the Post contains the JWS of a LogEvent as a Base64 encoded header, payload and signature

The LogEvent entry point assigns a globally unique LogEvent Identifier (per Section 2.1.8) to each LogEvent and returns it in the logEventId in its response.

Status Codes

201	LogEvent successfully logged
434	Signature Verification Failure
438	Unacceptable Algorithm
454	Unspecified Error
460	Bad LogEvent
461	LogEvent too big
462	LogEvent extension not on approved list
463	LogEvent extension on disallowed list

4.12.3.1.3 LogEvents by LogEvent Identifier

Retrieves a log event by its logEventId. Event is returned as a LogEventContainer (See Section 4.12.3.1.1.

HTTP method: GET

Resource name .../LogEvents/{logEventId}
Parameters:

© Copyright 2011-2022 National Emergency Number Association, Inc.

Name	Condition	Description
logEventId	MANDATORY	logEventId of the LogEvent data to to retrieve (see Section 2.1.8 LogEvent Identifier)

A successful response returns the LogEvent as a JWS

Status Codes

200 LogEvent found
404 Not found

4.12.3.2 Conversations

Returns an HTML formatted record suitable for human consumption of the text portion of a call, including all text sent by all parties.

HTTP method: GET

Resource name .../Conversations

Parameters:

Name	Condition	Description
callId	MANDATORY	Call ID of the call

A successful response includes the conversation as a string in the response body.

Status Code

200 Conversation found
404 Not found
454 Unspecified Error
464 No Text in this Call

4.12.3.3 LogEventIds

Retrieves LogEventIds. Use limit and start parameters for pagination.

HTTP method: GET

Resource name .../LogEventIds

Parameters:

Name	Condition	Description
limit	OPTIONAL	Maximum number of results to return

© Copyright 2011-2022 National Emergency Number Association, Inc.

Name	Condition	Description
start	OPTIONAL	First item in the page of results, as an ordinal 1-based integer.
callId	OPTIONAL	Call ID of the call
incidentId	OPTIONAL	Incident ID of the call

Status Codes

200 LogEvents found
404 Not Found
454 Unspecified Error

On a successful GET, a LogEventIdArray is returned:

LogEventIdArray

Name	Condition	Description
count	MANDATORY	Number of items in the array
totalCount	MANDATORY	Total number of items found
logEventIds	MANDATORY	Array of LogEvent identifiers

4.12.3.4 Call IDs

Returns a list of Call Identifiers associated with a specific Incident Tracking Identifier, occurred within a time range or within a specified geographic region.

HTTP method: GET

Resource name .../ListCalls

Parameters:

Name	Condition	Description
limit	OPTIONAL	Maximum number of results to return
start	OPTIONAL	First item in the page of results, as an ordinal 1-based integer.
incidentId	OPTIONAL	Incident ID of the call
startTime	OPTIONAL	Start time
endTime	OPTIONAL	End time
area	OPTIONAL	Area of interest

Status codes

200 Calls found

© Copyright 2011-2022 National Emergency Number Association, Inc.

404 Not Found
454 Unspecified Error
465 Bad Timestamp
466 EndTime occurs before StartTime
467 Bad Geoshape

On a successful GET, a CallIdArray is returned:

CallIdArray

Name	Condition	Description
count	MANDATORY	Number of items in the array
totalCount	MANDATORY	Total number of items found
callIds	MANDATORY	Array of Call IDs

4.12.3.5 Incident IDs

Returns a list of Incident Tracking Identifiers occurring within a time/date range. Returns a list of Incidents that occurred within a specified geographic region.

HTTP method: GET

Resource name .../IncidentIds

Parameters:

Name	Condition	Description
limit	OPTIONAL	Maximum number of results to return
start	OPTIONAL	First item in the page of results, as an ordinal 1-based integer.
startTime	OPTIONAL	Start time
endTime	OPTIONAL	End time
area	OPTIONAL	Area of interest

Status codes

200 Incidents found
404 Not found
454 Unspecified Error
465 Bad Timestamp
466 EndTime occurs before StartTime
467 Bad Geoshape

© Copyright 2011-2022 National Emergency Number Association, Inc.

On a successful GET, an IncidentIdArray is returned:

IncidentIdArray

Name	Condition	Description
count	MANDATORY	Number of items in the array
totalCount	MANDATORY	Total number of items found
incidentIds	MANDATORY	Array of Incident IDs

4.12.3.6 Agency IDs

Returns a list of agencies involved in a Call or an Incident.

HTTP method: GET

Resource name .../AgencyIds

Parameters

Name	Condition	Description
limit	OPTIONAL	Maximum number of results to return
start	OPTIONAL	First item in the page of results, as an ordinal 1-based integer.
incidentId	OPTIONAL	Incident ID of the call
callId	OPTIONAL	Call ID of the call

Status codes

200 Agencies found
404 Not found
454 Unspecified Error

On a successful GET, an AgencyIdArray is returned:

AgencyIdArray

Name	Condition	Description
count	MANDATORY	Number of items in the array
totalCount	MANDATORY	Total number of items found
agencyIds	MANDATORY	Array of Agency IDs

© Copyright 2011-2022 National Emergency Number Association, Inc.

4.12.3.7 LogEvent Types

This document creates a registry for LogEvent types. See Section 10.21.

Note: A description of which elements generate which LogEvent types will be described in a future version of this document.

This document defines the following EventTypes:

CallProcessLogEvent: Each element that is not call stateful, but handles a call logs the fact that it saw the INVITE or MESSAGE pass through by logging a CallProcessLogEvent event. There are no parameters to "Call Process". Elements that log CallProcessLogEvent also log the actual SIP message with CallSignalingMessageLogEvent.

CallStartLogEvent: Each element that is call stateful logs the beginning and end of its processing of a call, including non-interactive calls, with Start Call and End Call events. Elements that log CallStartLogEvent/CallEndLogEvent MUST also log the actual SIP message with CallSignalingMessageLogEvent for SIP parts of a call and GatewayCallLogEvent for TDM parts of a call. For CallStartLogEvent and CallEndLogEvent, the Timestamp MUST be the time the INVITE, MESSAGE, BYE or equivalents to these messages, or the final status code was received or sent by the element logging the event. Within CallStartLogEvent, a CallLogEvent object contains "direction", "standardPrimaryCallType", "standardSecondaryCallType", "localCallType" and "localUse". The "direction" member has one of two values, "incoming" or "outgoing", where "incoming" means a call received from the ESInet and "outgoing" means a call placed by, for example, a PSAP towards some caller. Optional "standardPrimaryCallType", "standardSecondaryCallType" and "localCallType" members MAY be included. The "standardPrimaryCallType" and "standardSecondaryCallType" members are limited to values found in the LogEvent Call Type Registry (see Section 10.23) "localCallType" can have any value defined locally. Optional "localUse" elements are also available (limited to 128 bytes each). When "CallStartLogEvent" is used with non-SIP interfaces, "to" and "from" members are used to capture the participants in the call.

CallEndLogEvent:. Each element that is call stateful logs the beginning and end of its processing of a call, including non-interactive calls, with Call Start and Call End events. Elements that log CallStartLogEvent/CallEndLogEvent MUST also log the actual SIP message with CallSignalingMessageLogEvent for SIP parts of a call and GatewayCallLogEvent for TDM parts of a call. For CallStartLogEvent and CallEndLogEvent, the Timestamp MUST be the time the INVITE, MESSAGE, BYE or equivalents to these messages, or the final status code was received or sent by the element logging the event. Within CallEndLogEvent, a CallEventLogEvent object contains "direction", "standardPrimaryCallType", "standardSecondaryCallType", "localCallType" and "localUse" as

© Copyright 2011-2022 National Emergency Number Association, Inc.

defined above in CallStartLogEvent. When CallEndLogEvent is used with non-SIP interfaces, "to" and "from" members are used to capture the participants in the call.

RecCallStartLogEvent is identical to CallStartLogEvent but is logged by the Logging Service (SRS) and the client (SRC) for the SPIREC recording session.

RecCallEndLogEvent is identical to CallEndLogEvent but is logged by the Logging Service (SRS) and the client (SRC) for the SPIREC recording session.

CallTransferLogEvent: When a call is transferred, the transfer is logged by the transferor (the entity that had the call prior to transferring it). The transfer target URI is logged in a target member. Elements that log CallTransferLogEvent MUST also log the actual SIP targetCallIdSIP member that contains the SIP CallId of the new session with the transfer target, when known. Note that the PSAP may not know this CallId, but the bridge would.

RouteLogEvent: A proxy server that makes routing decisions (ESRPs or other SIP proxy servers in the path of the call) logs the route it selected with the RouteLogEvent EventType. The LogEvent contains the URI to which it decided to send the call (encoded in a "recipientUri" member), an optional text string "cause" stating why it chose the route, the policy owner (in a "policyOwner" member), policy type (in a "policyType" member), policy ID if policyType is "OtherRoutePolicy" (in a "policyID" member), policy queue name if policyType is "OriginationRoutePolicy" or "NormalNextHopRoutePolicy" (in a "policyQueueName" member), and the rule ID (in a "ruleId" member).

MediaStartLogEvent: MediaStartLogEvent contains information about one call medium (voice, video, or RTT/MSRP text). The media event includes a text string "sdp"member that contains an RFC 2327 Session Description Protocol [12] description of the media codecs as negotiated. The MediaStartLogEvent event MUST include one or more "mediaLabel" members that MUST match the SDP labels [99] if they exist. More than one MediaStartLogEvent can occur for a call. Recorded media streams include integral time reference data within the stream. This event is logged by any media anchor (call recipient for an emergency call, caller for a callback, bridge, or BCF if the BCF anchors media) when at the start of media reception or transmission as appropriate. A "direction" member has one of two values: "incoming" or "outgoing".

MediaEndLogEvent: MediaEndLogEvent signals that media streams stopped. The MediaEndLogEvent MUST include one or more "mediaLabel" members that must match the SDP labels in the corresponding MediaStartLogEvent. More than one MediaEndLogEvent (with different "mediaLabel"s) MAY occur for a call. This event is logged by any media anchor (call recipient for an emergency call, caller for a callback, bridge, or BCF if the BCF anchors media) for the communication session media. A "mediaQualityStats" member contains tags that give QoS statistics about the media stream. The content of

© Copyright 2011-2022 National Emergency Number Association, Inc.

"mediaQualityStats" MUST be a "SessionReport" element from RFC 6035 [43]. "mediaQualityStats" SHOULD be supported by all media anchors.

RecMediaStartLogEvent and RecMediaEndLogEvent are identical to MediaStartLogEvent/MediaEndLogEvent but apply to the SIPREC recording session. Both the SRC and SRS log RecMediaStartLogEvent/RecMediaEndLogEvent. If an entity receives a media stream that it transcodes to another stream, including receiving TTY tones as audio, the entity transcoding creates a SIPREC recording stream for the transcoded media it creates, and logs RecMediaStartLogEvent for it. The "mediaLabel" members MUST be the same as those in the MediaStartLogEvent/MediaEndLogEvent so that matching of streams is possible. If the SRC mixes audio from multiple streams, the mediaLabel is composed from the mediaLabels used in the originating streams, concatenated with a "+" between them. A "mediaTranscodeFrom" member is used in this case containing the RFC 4575 [40] label of the original incoming stream. Absence of the tag indicates no transcode is performed. For TTY received as audio, the recorded stream would be Real-time Text.

RecordingFailedLogEvent: RecordingFailedLogEvent indicates that the entity logging this event attempted to record media, but the media recording mechanism failed. This event contains an SDP description of the media that failed to be recorded in a "sdp" member, and "reasonCode" and "reasonText" parameters that specify why recording could not complete. "reasonCode" MUST be a value from the IANA LoggingServiceMediaErrorReasonCodes registry. The Session Recording Client in a SIPREC media recording session is responsible for logging this event.

MessageLogEvent: A SIP Message is logged with a MessageLogEvent. Elements that log Message MUST also log the actual SIP message with CallSignalingMessageLogEvent. The text of the message is included as a "text" parameter. A "direction" member has one of two values: "incoming" or "outgoing".

AdditionalAgencyLogEvent: When an agency becomes aware that another agency may be involved, in any way, with a call, it MUST log an AdditionalAgencyLogEvent. The AdditionalAgencyLogEvent includes an "agencyId" member which is an Agency Identifier (see Section 2.1.1). Among other uses, this event is used by PSAP management to query all Logging Services that may have records related to a call or incident.

IncidentMergeLogEvent: More than one call may be received about the same real world Incident. Since each call is initially assigned its own Incident Tracking Identifier, the Agency SHOULD merge them by assigning the subsequent call to the first call's Incident Tracking Identifier so that it's clear that both calls are about the same Incident. Also, while handling two incidents, it may become apparent later that the incidents are in fact, the same real world Incident. The Ids are merged with IncidentMergeLogEvent. The IncidentMergeLogEvent record contains the IncidentId of the incorrectly assigned incident

© Copyright 2011-2022 National Emergency Number Association, Inc.

in the "incidentId" member in the header field of the log record, and the Incident Id of the actual Incident in a "IncidentIdMerge" member. After a merge, the Id in the "incidentIdMerge" member SHOULD be used to refer to this Incident. Note that other agencies may not know that the Incidents are being merged, and therefore could log events against the originally assigned IncidentId.

IncidentUnMergeLogEvent: When a IncidentMergeLogEvent is found to have been done in error, IncidentUnMergeLogEvent will undo the operation. The IncidentUnMergeLogEvent record contains the IncidentId of the Merged incident in the "incidentId" member in the header field of the log record, and the IncidentId of the other Incident in an "incidentIdUnmerge" member.

IncidentSplitLogEvent: When an agency creates a new Incident by cloning the data from an existing Incident, and then assigning a new Incident Tracking Identifier to the new one, it logs the IncidentSplitLogEvent. IncidentSplitLogEvent requires the agency splitting the incident to create two records, one with the old Incident Id in the header field and the new Incident Id in the tag, and another IncidentSplitLogEvent record with the new Incident Id in the header field and the old one in the tag. The old or new Id is included in an "incidentId" member, which contains the Id and a "type" attribute that specifies whether this tag contains the "old" Id or the "new" Id.

IncidentLinkLogEvent: Incidents are linked when two different incidents are not the same real world event but are related in some way. The IncidentLinkLogEvent record contains the Incident Tracking Identifier of the new Incident in the "incidentId" member in the header field, and the Incident Tracking Identifier of the original Incident being linked to in a "incidentIdLinked" member. The "relationship" member specifies the relationship between the incidents. Values include "parent", "child", "peer", and "unspecified". For "parent" and "child", the incidentId in the header field is the one described by the "relationship" member.

IncidentUnLinkLogEvent: When a IncidentLinkLogEvent is found to have been done in error, IncidentUnLink will undo the operation. The IncidentUnLinkLogEvent record contains the IncidentId of the Linked incident in the "incidentId" member in the header field of the log record, and the IncidentId of the other Incident in an "IncidentIdunlinkedFrom" member.

IncidentClearLogEvent: When an agency finishes its handling of an Incident, it logs a IncidentClearLogEvent record. Other agencies may still be processing the Incident.

IncidentReopenLogEvent: If an agency needs to LogEvents on an Incident for which it has logged a IncidentClearLogEvent, it logs a IncidentReopenLogEvent.

© Copyright 2011-2022 National Emergency Number Association, Inc.

LostQueryLogEvent: Both the element that queries the ECRF/LVF and the ECRF/LVF itself generate a LostQueryLogEvent. The LogEvent includes the entire LoST query in the "queryAdapter" member. A "direction" member tag has one of two values: "incoming" or "outgoing". The ECRF/LVF will obtain the CallId and IncidentId from the LoST extension defined in Section 3.4.10.4. A "queryId" member is used to relate the request to the response. The id is generated locally, MUST be globally unique, and it is suggested that it be of the form: "urn:emergency:uid:queryid: 'globally unique id'". If the element is logging a malformed query it has received, it includes it in a "malformedQuery" member.

LostResponseLogEvent: Both elements that query the ECRF/LVF, and the ECRF/LVF itself generate the LostResponseLogEvent. The entire response is logged using "responseAdapter" member. Malformed, invalid, or responses not received from the server are logged in a "responseStatus" member that contains a status code from the Status Codes Registry (Section 10.29). A "direction" member has one of two values: "incoming" or "outgoing". A "responseId" member is used to relate the request to the response, and MUST match the id used in the LostQueryLogEvent. If the element is logging a malformed response it has received, it includes it in a "malformedResponse" member.

CallSignalingMessageLogEvent: Call Signaling (e.g., SIP) messages are logged with the CallSignalingMessageLogEvent. The entire message is included in a "text" member. A "direction" member has one of two values: "incoming" or "outgoing". An element MUST always log messages it receives (with "direction" set to "incoming"). If an element sends a signaling message as a result of an incoming logged message, it need only log the outgoing message (with "direction" set to "outgoing") if it changes any part of the signaling message. An element MUST log outgoing messages it originates. A "protocol" member indicates the protocol. Absence of the "protocol" member defaults to "sip". A registry of protocol values is defined in Section 10.22.

SipRecMetadataLogEvent: The SRS MUST create LogEvents for any metadata received via the SIPREC metadata interface (RFC 7865) [117]. It does this by logging a SIPRECMetadataLogEvent to itself. The metadata included is a "siprecMetadataText" tag. The SRS MUST fill in the header fields for which the values are known, such as the CallId and IncidentId supplied by the Session Recording Client. The sipCallId in the header field will be set to the SIP callId from the communication session, not the SIP callId from the recording session.

NonRtpMediaMessageLogEvent: Some media, for example MSRP, do not use RTP to transport the media. The messages that transport this media are logged with NonRtpMediaMessageLogEvent. The entire message is included in a "text" member. A "direction" member has one of two values: "incoming" or "outgoing". An element MUST always log messages it receives (with "direction" set to "incoming"). If an element sends a media message as a result of an incoming logged message, it need only log the outgoing

© Copyright 2011-2022 National Emergency Number Association, Inc.

message (with "direction" set to "outgoing") if it changes any part of the media message. An element MUST log outgoing messages it originates. A "protocol" member indicates the protocol. Absence of the "protocol" member defaults to "sip". A registry of protocol values is defined in Section 10.22.

AliLocationQueryLogEvent: An LSRG [114] logs the query it sends to or receives from an ALI server with the AliLocationQueryLogEvent. An LPG also uses this LogEvent when it receives an ALI query from the legacy PSAP. The text of the query is included in a "text" member, and any message delimiter control characters such as STX/ETX are not included. The CallId and IncidentId MAY be left blank if they are not known by the LSRG (because the LSRG is outside the ESInet and does not assign these IDs). A "directionValuesCode" member has one of two values: "incoming" or "outgoing". A "queryId" member is used to relate the request to the response. The id is generated locally, MUST be globally unique, and it is suggested that it be of the form: "urn:emergency:uid:queryid:'globally unique id'".

AliLocationResponseLogEvent: An LSRG MUST log the response it sends to or receives from its query to an ALI server with the AliLocationResponseLogEvent. An LPG MUST also use this LogEvent when it responds to an ALI query from the legacy PSAP. The text of the response is included in a "text" member, and any message delimiter control characters such as STX/ETX are not included. Malformed, invalid, or responses not received from the server are logged in a "responseStatus" member that contains a status code from the Status Codes Registry (Section 10.29). A "direction" member has one of two values: "incoming" or "outgoing". A "responseId" member is used to relate the request to the response and MUST match the id used in the AliLocationQueryLogEvent.

MalformedMessageLogEvent: An element that receives a malformed SIP message logs it with the MalformedMessageLogEvent. The malformed message is included in a "text" member. An "ipAddress" member is included, which contains the IP address of the sender of the message. An optional "eventExplanationText" member contains a human-readable explanation of why the SIP message was flagged as malformed. If the element believes it is under a DOS attack, then it MAY not log all malformed messages to avoid overloading the Logging Service.

EidoLogEvent: Any element that sends or receives an Emergency Incident Data Document [111] MUST log it with the EidoLogEvent. If the EIDO is sent by value, the value is logged in a "body" member. If an EIDO is sent or received by reference, the EIDO URI MUST be logged with a "reference" member. When the URI is dereferenced, another EIDOLogEvent MUST be created with the "reference" and "body" by both the client and server. A "direction" member has one of two values: "incoming" or "outgoing".

DiscrepancyReportLogEvent: Any element that sends or receives a Discrepancy Report, or that sends or receives an update (Status, Resolution, etc.) for one, logs what it sent or

© Copyright 2011-2022 National Emergency Number Association, Inc.

received with the DiscrepancyReportLogEvent. The body of the report or response is included in a "contents" member. A "direction" member has one of two values: "incoming" or "outgoing". A "type" member identifies the name of the Discrepancy Reporting web service function that was called to make the report or response (DiscrepancyReportRequest, StatusUpdateResponse, etc.). See the Discrepancy Reporting section of this document for the full list of function names and details.

ElementStateChangeLogEvent: When an element sends a notification of state change as described in the Element State section of this document, it MUST log the ElementStateChangeLogEvent. The event contains the body of the notification message in a "notificationContents" member. Elements that receive changes in ElementState MAY log receipt of such changes. The new state is logged with "StateChangeNotificationContents" member. The element ID (FQDN) of the element whose state changed is logged in the "affectedElementId" member. This tag is optional if the element that provides the state change is the element whose state is changed. A "direction" member has one of two values: "incoming" or "outgoing". Note that a Call Identifier, SIP Call Id, and Incident Tracking Identifier usually won't be available for an ElementStateChangeLogEvent. Devices that have proprietary interfaces may implement ElementStateChangeLogEvent even though they may not emit the notification defined in this document. Their states SHOULD be mapped to the closest state defined by the notification and logged with that state using ElementStateChangeLogEvent.

ServiceStateChangeLogEvent: When a Service sends a notification of state change as described in the Service State section of this document, which includes Security Posture, it MUST log the ServiceStateChangeLogEvent. Elements that receive changes in serviceState MAY log receipt of such changes. The new state is logged with "newState" member for service state changes and in the "newSecurityPosture" member for security posture changes, if Security Posture is supported by the service. The service ID (FQDN) of the service whose state changed is logged in the "affectedServiceIdentifier" member. A "direction" member has one of two values: "incoming" or "outgoing". Note that a Call Identifier, SIP Call Id, and Incident Tracking Identifier usually won't be available for a ServiceStateChangeLogEvent.

AdditionalDataQueryLogEvent: A query for Additional Data MAY be logged with the AdditionalDataQueryLogEvent. The URI the request was sent to is logged in a "uri" member. The event contains the body of the query in a "text" member. Logging queries at the client is optional but is RECOMMENDED because it shows the time lapse between query and response and provides for better troubleshooting. A server for AdditionalData that is located inside an ESInet, or LNG, or LSRG operated by, or on behalf of, a 9-1-1 Authority, MUST log all queries it receives. A "direction" member has one of two values: "incoming" or "outgoing". A "queryId" member is used to relate the request to the response. The id is

© Copyright 2011-2022 National Emergency Number Association, Inc.

generated locally, MUST be globally unique, and it is suggested that it be of the form: "urn:emergency:uid:queryid:'globally unique id'".

AdditionalDataResponseLogEvent: Any Additional Data that is retrieved by a client MUST be logged using the AdditionalDataResponseLogEvent. The body of the retrieved data is included in "text" members, one per block of Additional Data. Malformed, invalid, or responses not received from the server are logged in a "responseStatus" member that contains a status code from the Status Codes Registry (Section 10.29). A server for AdditionalData that is located inside an ESInet, and an LNG, LPG, or LSRG operated by, or on behalf of, a 9-1-1 Authority, MUST log all responses it sends. A "direction" member has one of two values: "incoming" or "outgoing". A "queryId" member is used to relate the request to the response and MUST match the id used in the AdditionalDataQueryLogEvent.

LocationQueryLogEvent: A HELD dereference request (RFC 6753) [55] or SIP Presence SUBSCRIBE message (RFC 3856) [25] MAY be logged with the LocationQueryLogEvent. The URI the request was sent to is logged in a "uri" member. The body of the request or SUBSCRIBE is included in a "text" member. Logging these is OPTIONAL at the client and REQUIRED at the server if the server is located inside an ESInet, or is an LNG or LSRG operated by, or on behalf of, a 9-1-1 Authority. A "direction" member has one of two values: "incoming" or "outgoing". A "queryId" member is used to relate the request or subscription to the response or notifications. The id is generated locally, MUST be globally unique, and it is suggested that it be of the form: "urn:emergency:uid:queryid:'globally unique id'".

LocationResponseLogEvent: A HELD dereference response, a SIP Presence NOTIFY message, and a re-INVITE with a new location are logged with the LocationResponseLogEvent message. The body of the response or message is included in a "text" member. Malformed, invalid, or responses not received from the server are logged in a "responseStatus" member that contains a status code from the Status Codes Registry (Section 10.29). All clients and servers, if the server is located inside an ESInet, or is an LNG or LSRG operated by, or on behalf of, a 9-1-1 Authority, MUST log responses. A "direction" member has one of two values: "incoming" or "outgoing". A "responseId" member is used to relate the request or subscription to the response or notifications and MUST match the id used in the LocationQueryLogEvent.

CallStateChangeLogEvent: This is used by an element to log a state change, such as logging an "answered" event by a device. The new state is included in a "state" member. The CallId, IncidentId, and sipCallId in the header field are from the emergency call whose state has changed. For state changes that involve another "leg" of a call, such as AddParty, a "legCallId" member contains the call id of that leg. If the leg is a SIP leg, this Id is the SIP Call Id of the leg otherwise it may be another identifier for that call. CallStateChangeLogEvent MUST be logged by all elements that change the state of the call,

© Copyright 2011-2022 National Emergency Number Association, Inc.

which would include a bridge and all entities within the ESInet that request bridge actions when an emergency call is on a bridge. A "direction" member has one of two values: "incoming", meaning the element logging the state change received a message or other notice that changed the state; and "outgoing", meaning this element caused the state change. If the target involved in the state change is not the element identified in the header field, the identifier of the target whose state changed must be included in a "targetId" member. If the target is a SIP device, this must be the sip URI of the target. An optional "changeReason" member contains the reason why the state changed. The content of this tag is not standardized at this time. A registry for these call states is defined in Section 10.24.

GatewayCallLogEvent: This is used by an LNG, LPG, or LSRG to log a call entering or leaving on a legacy interface. It contains the following parameters which are OPTIONAL, but MUST be included if known:

- portTrunkGroup – the port or trunk group
- pAni – 10-digit number when LNG or LSRG handles a call from a legacy wireless or legacy VoIP network, or the pANI an LPG creates.
- digits – what the LNG/LSRG received from the network (8, 10, or 20 digits) or what the LPG sent. If 20 digits, the first 10 are the calling party id, and the second 10 are the pANI, separated by a comma.
- direction – "incoming" or "outgoing"
- signalingProtocol – "SS7" or "CAMA"
- legacyCallId

HookflashLogEvent: An LPG logs a "hookflash" event with the HookflashLogEvent. An identifier for the line on which the event occurred is included in a "lineId" member, which is OPTIONAL but MUST be provided if known. It is not used when already logged as part of a GatewayCallLogEvent.

LegacyDigitsLogEvent: An LPG logs DTMF or MF digits with the LegacyDigitsLogEvent. A "sentReceived" member, with values of "sent" or "received", identifies the direction of the digits. A "type" member, with a value of "DTMF" or "MF" identifies the type of digits that were received. "digits" carries the digit or digits that were transmitted or received. These are not used when already logged by GatewayCallLogEvent (such as sending pANI digits at an LPG).

AgentStateChangeLogEvent: An element logs a change in agent device state with the AgentStateChangeLogEvent. There are two tags "primaryAgentState" and secondaryAgentState". "primaryAgentState" has two values: Available and Not Available. A registry for secondary agent device states is defined, see Section 10.21. If the device whose state has changed is not the element identified in the header field, the identifier of

© Copyright 2011-2022 National Emergency Number Association, Inc.

the device MUST be included in a "deviceID" member. All elements supporting agents MUST support the "primaryAgentState"; "secondaryAgentState" support is OPTIONAL.

Several of these secondary states (e.g., Active and Hold) make sense with both Available and Not Available primary states.

QueueStateChangeLogEvent: A queue manager MUST log a change in the state of the queue with the QueueStateChangeLogEvent. The event contains the body of the notification message in a "notificationContents" member. Elements that receive changes in QueueState MAY log receipt of such changes and MUST log a state change to "unreachable". The queue ID whose state changed is logged in the "queueId" member. A "direction" member has one of two values: "incoming" or "outgoing". Note that a Call Identifier, SIP Call Id, and Incident Tracking Identifier usually won't be available for a QueueStateChangeLogEvent.

KeepAliveFailureLogEvent: The OPTIONS request is the "keep alive" mechanism specified in this document (Section 3.1.2.3). An element that gets a normal response to its OPTIONS request does not log the response. Malformed, invalid, or responses not received from the other element MUST be logged in a "responseStatus" member that contains text and a status code from the Status Codes Registry (Section 10.29). There is a TimeOut status in that registry that is used for a timeout failure of OPTIONS.

RouteRuleMsgLogEvent: The LogMessageAction object (see Section 3.3.3.2.4 Log Message Action) generates a RouteRuleMsgLogEvent containing the policy owner (in a "policyOwner" member), policy type (in a "policyType" member), policy ID if policyType is "OtherRoutePolicy" (in a "policyID" member), policy queue name if policyType is "OriginationRoutePolicy" or "NormalNextHopRoutePolicy" (in a "policyQueueName" member), the rule ID (in a "ruleId" member), rule priority (in a "priority" member), and the contents of the action's "message" member if present (in a "message" member).

PolicyChangeLogEvent: Policy changes are logged in a PolicyChangeLogEvent. The type of the Policy is specified in a "type" member. "queueName" and "policyId" are provided as appropriate and the owner is specified in an "owner" member. The type of change is specified in a "changeType" member, and has one of three values: "CREATE", "UPDATE", or "DELETE". "CREATE" is used when the policy store did not have a policy with the "policyType", "policyId" or "policyQueueName", "UPDATE" is used when it does. The policy being "CREATE"d or "UPDATE"d is specified in a "policyContent" member. The name of the Policy Store, or the URL of the Policy Store web service, is specified in a "policyStoreId" member. The name of the application used to make the change is specified in a "policyEditor" member.

© Copyright 2011-2022 National Emergency Number Association, Inc.

VersionsLogEvent: Records the response to a web service Versions request (See Section 2.8). A "source" member has the URL used to query versions and the "response" member has the response received.

SubscribeLogEvent: When a subscription request is processed for any defined Event Package, the transaction is logged with SubscribeLogEvent. A "package" member is a selection from the Event Package Registry (See Section 10.35). A "peer" member contains the URI or FQDN of the other party. An array of type/value "parameter" members contain any parameters in the subscribe. The "expiration" member contains the final expiration time negotiated. A "response" member records the response code the subscription received/sent. The "purpose" flag is set to "initial" for a new subscription, "refresh" for a refresh of an existing subscription, and "terminate" for a terminated subscription. The Server MUST log this event, the client MAY log. A "direction" member tag has one of two values: "incoming" or "outgoing". A "subscriptionId" member is used to relate the correlate transactions on this subscription. The id is generated locally, MUST be globally unique, and it is suggested that it be of the form: "urn:emergency:uid:subid:'globally unique id'".

A registry for LogEvents is defined. See Section 10.21. A registry for the Event Package is defined, see Section 10.35.

Note: A description of which elements generate which LogEvent types will be described in a future version of this document.

4.12.3.8 Instant Recall Recorder

The ability to quickly review current or recent emergency communications content is important. The Logging Service's Web Service interface supports this capability with the query, retrieval, and streaming media functions described in Section 4.12. This interface supports recall of all defined media types. A client application may use these functions to retrieve media for display or playback. The client is expected to impose any additional limitations required by local policy, such as limiting recall to communications the user has handled, to specific communications types, and/or limiting the time period from which recent communications can be recalled. The client is also responsible for providing functionality that allows the user to navigate within and between recalled communications. Access to media for instant recall is subject to the same security restraints as all log records. The PSAP may impose additional constraints as to which agents may access media.

4.12.3.9 LogEventReplicator

Devices or services may be created that use LogEvents to provide some benefit. An example is a readerboard that shows a call queue. Such devices may wish to receive a clone of the LogEvent stream going to the Logging Service. A LogEventReplicator has

© Copyright 2011-2022 National Emergency Number Association, Inc.

interfaces identical to LogEvent (Section 4.12.3). It can take a stream of LogEvents on its input port(s) and replicate them to each of its provisioned output ports. One of the output ports may be connected to the Logging Service, in which case all FEs that log would send their LogEvents to the replicator, which would copy them to the Logging Service and the other devices connected to the replicator. The replicator may be integrated into the Logging Service, may be stand-alone, or may be integrated into another FE.

The replicator MUST replicate LogEvents exactly as they were received without modifying any field. For example, if a replicator inserted its own ElementID or Timestamp in the header field, it would destroy the original data the elements subscribing to the event would need.

Replicators may have filtering capability to restrict which events are sent to which ports, but such filtering is not otherwise standardized. Each event received by the replicator MUST be sent to each of the output ports, subject to such filtering, if implemented. One of the output ports is designated the "master" port. When a transaction is started on the input port, the replicator starts the transaction on all of its output ports. Whatever response is returned from the master port is used as the response from the replicator to the input port. All other responses are ignored. If the Logging Service is connected to a replicator output port, normally it would be on the master port.

4.12.4 Roles and Responsibilities

Any agency, including a PSAP, may run its own Logging Service. The ESInet may have one or more Logging Services. All agencies and NG9-1-1 functional elements MUST have access to a conformant Logging Service and log all relevant events in that service. Media are recorded as specified in Section 4.12, with recording at more than one point in the call path desirable. Recording of media at the BCF can be substituted for recording of media at the endpoints if the BCF is always in the path of all media. Recording media is subject to legal and privacy restrictions that may govern where media is recorded and who has access to such recordings.

4.12.5 Operational Considerations

Because events and media related to an Incident may be logged in several different Logging Services during the life of the Incident, it will sometimes be necessary to query multiple Logging Services to reconstruct what happened. Similarly, a Logging Service may be in the ESInet and shared among several agencies. This implies the need for policies and agreements between different jurisdictions to control what can be retrieved, and under what circumstances. These policies must find a balance between the desire to protect potentially sensitive media, and the need to provide access to those media for legal reproduction and troubleshooting purposes.

© Copyright 2011-2022 National Emergency Number Association, Inc.

It is anticipated that the same media may be recorded in more than one Logging Service along the call chain, thus providing some redundancy. It is not anticipated that the same LogEvents will be logged in more than one Logging Service; an element will LogEvents to the Logging Service that serves its own network.

The data stored in a Logging Service contain a wealth of raw statistical information that can be collated and compared with data from other systems and Logging Services to provide valuable insights into how the NG9-1-1 service is performing. Providing access to these data for such analysis will be valuable because that analysis can guide resource allocation to support continual improvement of services. Policies and agreements will need to be established to facilitate appropriate sharing of these data.

4.13 Forest Guide

The ECRF and LVF infrastructure make use of Forest Guides as defined in RFC 5582 [47]. A server that does not answer a query can refer to a Forest Guide to determine the response.

4.13.1 Functional Description

The following definitions are adapted from those in RFC 5582, used with permission of the authors:

- Authoritative ECRF/LVF: A LoST server that can provide the authoritative answer to a particular set of queries (e.g., covering a set of civic labels or a particular region described by a geometric shape). An authoritative ECRF/LVF may redirect or forward a query to another authoritative ECRF/LVF within the tree.
- Child: An ECRF/LVF that is authoritative for a sub-region of another authoritative ECRF/LVF. A child can in turn be a parent for another authoritative ECRF/LVF.
- (tree node) cluster: A node cluster is a group of ECRFs that all share the same mapping information and return the same results for queries. Clusters provide redundancy and share query load. Clusters are fully meshed (i.e., they all exchange updates with each other).
- Coverage region: The coverage region of an authoritative ECRF/LVF is the geographic region within which the ECRF/LVF is able to authoritatively answer mapping queries. Coverage regions are generally, but not necessarily, contiguous and may be represented as either a subset of a civic address or a geometric object.
- Forest Guide (FG): A Forest Guide has knowledge of the coverage region of trees for a particular top-level service.
- Parent: A LoST server that covers the region of all of its children. A LoST server without a parent is a root authoritative ECRF/LVF.
- Tree: A self-contained hierarchy of authoritative mapping servers for a particular service. Each tree exports its coverage region to the Forest Guide.

© Copyright 2011-2022 National Emergency Number Association, Inc.

Given a query to an area outside its coverage area, an ECRF/LVF may have the coverage regions of other ECRF/LVFs to which it could refer a query, or it would refer to a Forest Guide. In NG9-1-1, each state is nominally a tree, with local ECRF/LVFs as the children. The top of the tree is often a state ECRF/LVF. There is a National Forest Guide that has knowledge of these trees. The National Forest Guide exchanges mappings with other National Forest Guides. A state coverage region, exported to the National Forest Guide, could be the civic state element, and a polygon representing the state boundary.

4.13.2 Interface Description

The National Forest Guide maintains a LoST interface, as described in Section 3.4, for query resolution. It also maintains a LoST-sync interface defined in RFC 6739 [79] for updating its coverage regions. The LoST-sync interface is used for both state ECRF/LVF interfaces and other National Forest Guides. The National Forest Guide only serves "urn:service:sos", "urn:emergency:service:sos", and "urn:emergency:service:responder". It may be able to refer to other Forest Guides for services other than these. The National Forest Guide may interchange coverage with other National Forest Guides.

A Forest Guide provides gap/overlap coverage analysis as described for ECRFs in Section 4.3.5 and provides the same notification service described.

The Forest Guide MUST implement the server-side of the ElementState event notification package.

4.13.3 Data Structures

The Forest Guide has one or more civic data structures and one or more GML polygons (set) representing the state coverage region. It also maintains coverage regions for other countries in a similar manner.

4.13.4 Roles and Responsibilities

The Forest Guide SHOULD be managed nationally (agency not yet identified) and MAY evolve to an entity more representative of all public safety agencies or covering more than one nation (e.g. Canada and the U.S. could share a Forest Guide). As described in RFC 5582, there is no requirement that a Forest Guide be "official" or national government sanctioned. The operators of the constituent ESInets can decide whether or not to trust that any entity purporting to be a Forest Guide actually does provide the service, and so provide their coverage and mappings, and query it for out-of-area data. Although this document envisions that there will be a single authoritative Forest Guide for each country (or multiple countries), there could in fact be more than one and as long as the constituent ESInets contribute their data, it could be used. State ECRF and LVF operators SHALL arrange for their coverage regions to be provisioned in a Forest Guide. Forest Guide

© Copyright 2011-2022 National Emergency Number Association, Inc.

operators SHALL maintain well-known contact information so that other Forest Guides can arrange to exchange their coverage regions and mappings. Until a Forest Guide is available, State ECRF and LVF operators SHOULD exchange coverage and mapping data with other ESInet providers.

4.13.5 Operational Considerations

The Forest Guide idea is specifically designed so that there is no global "root" Forest Guide. This means that the National Forest Guide will have to develop policies for its own operation when identifying the authoritative Forest Guide for another country or area. Specifically, it can be expected to have to deal with disputed territory, where more than one National Forest Guide claims they are authoritative for the same area.

4.13.6 Security Considerations

Since the Forest Guide could be a bottleneck in the routing or transfer of emergency calls that are not initially presented to the appropriate ESInet, it is an attractive attack target. For this reason, there SHALL be both internal and external Forest Guides. The internal Forest Guide is accessible to ESInets and only allows queries from entities inside those ESInets. The external Forest Guide is public and allows queries from any source. When it is under stress, the internal Forest Guide MAY refuse queries from any entity for which it does not have existing entries (nominally state level ECRFs, and other Forest Guides). For this reason, queriers needing routes for emergency calls SHOULD always query their local ECRF using recursion, which will result in obtaining the correct mapping, possibly involving the internal Forest Guide as part of the query resolution process. When not under stress, the internal Forest Guide MAY answer queries from other entities, but such queries would result from misconfiguration in the querier, and management action to identify such problems may be undertaken by the Forest Guide operator. State ESInets and even large OSPs SHOULD maintain a local copy of the Forest Guide to use if they are unable to access the Forest Guide. The Forest Guide SHOULD provide an RFC 6739 LoST-sync feed for these local replicas.

4.14 DNS

All elements identified by hostnames MUST have corresponding Domain Name Service (DNS) records as specified in STD13 (RFC 1034) [74] in the global public DNS. All elements connected to the ESInet MUST have local DNS resolvers to translate hostnames they receive to IP addresses. Since the ESInet must continue to work in the face of disasters, DNS servers must be highly redundant. When a caching DNS resolver in the ESInet cannot refresh an expired cached resource record in response to a query because the authoritative DNS server is not available, it SHOULD reuse the stale cached resource record as though the cached resource record's TTL is 1 second, as described in Section 4 of RFC 8767 [220].

© Copyright 2011-2022 National Emergency Number Association, Inc.

DNSSEC (RFC 4035) [118] MUST be deployed in authoritative DNS servers, especially those resolving names found in external ECRF/LVFs.

A domain that has SIP elements within the domain MUST have an SRV record RFC 2782 [75] for a SIP service for the domain, and any of its subdomains that may appear in a URI.

Placing a LoST query always requires resolution of an Application-Unique String (AUS), which is in the form of an FQDN via U-NAPTR (RFC 4848 [154]), and U-NAPTR resolution may also be required to obtain the URI for a LIS (per RFC 5986) [155].

4.15 Service/Agency Locator

The ESInet will connect to many services and public safety agencies. A directory ("white pages" and "yellow pages") of agencies, together with key information about the service or agency, is the function of the Service/Agency Locator. The Service/Agency Locator is a distributed database. There are several mechanisms by which the Service/Agency Locator can be searched to locate a specific service or agency. One primary way to search the Service/Agency Locator is by name. The Service/Agency Locator provides a name (white page) search function, with wild cards, to find a specific service or agency. The search by name is more useful for agencies than services. The name that is searched comes from the "org" field of the Agency jCard that is returned in the Service/Agency Locator Record. Another method to search is by location and agency type.

A Service/Agency Locator Service is provided in the ESInet. Every service as defined in Section 2.1.5 and every Public Safety Agency connected to the ESInet is listed in the Service/Agency Locator. The Service/Agency Locator has two components:

a) A Service/Agency Locator Record Store (SALRS) which holds the actual data record for the service or agency;
b) A search component, which uses the ECRF and a LoST query to find a given service or agency by type and location.

A service/agency locator record is identified by a URI whose domain is an SALRS. The URI can be presented to an SALRS that will respond with the record. The ECRF returns the URI (see Section 4.15.2.

Each FE in the Service/Agency Locator MUST implement the server-side of the ElementState event notification package. The Service/Agency Locator FE MUST promptly report changes in its state to its subscribed elements.

The set of Service/Agency Locator FEs within an ESInet MUST implement the server-side of the ServiceState event notification package for the Service/Agency Locator. Since the Service/Agency Locator Service is typically a state-wide service it is RECOMMENDED that the state level Service/Agency Locator subscribe to ElementState for each Service/Agency

© Copyright 2011-2022 National Emergency Number Association, Inc.

Locator FE within the state and provide a single Service/Agency Locator ServiceState notifier for the entire state.

4.15.1 Service/Agency Locator Record Store

A Service/Agency Locator Record Store is a web service that, when presented with a service/agency locator URI, returns the service/agency locator record. An HTTPS GET on the URI is used to retrieve a record from the Record Store. The querier MUST use credentials traceable to the PCA to create the TLS connection, and the credential and its corresponding agency type and role may influence which information is returned.

The SALRS may be operated by the agency itself, the ESInet operator may operate an SALRS for the entire ESInet, or any other party may operate an SALRS. Every service and every agency MUST have a record stored in at least one SALRS, with the URI for that record stored in the ECRF that serves the service or agency.

4.15.2 Service/Agency Locator Search by Location

The ECRF is used for a Service/Agency Locator search function. For this purpose the service URNs for all service and agency types are defined, starting with "urn:emergency:service:serviceagencylocator" and followed by a Service Name or agency type.

For example, to find the service or agency locator record for the police department that serves the city of Wonderville, in Sunshine County, Iowa, a client sends a LoST FindService query to the ECRF. The query is constructed as follows:

- a <service> element set to "urn:emergency:service:serviceagencylocator.police"
- a <location> element constructed as follows:
  - a "profile" attribute set to "civic
  - a <civicAddress> element containing:
    - a <country> element set to "US"
    - an <A1> element set to "IA"
    - an <A2> element set to "Sunshine"
    - an <A3> element set to "Wonderville"

The ECRF returns a LoST findservice response. The response contains a <mapping> element that contains a URL within a <uri> element. In this example, resolving the returned URL results in the SALRS returning the service/agency locator record for the Wonderville police department. Note that if the ECRF is aware of more than one matching agency, it returns at least one <mapping> element for each agency.

Service Names come from the Service Names registry (Section 10.11). The agency types are taken from the urn:emergency:service:responder registry (Section 10.5) and the

© Copyright 2011-2022 National Emergency Number Association, Inc.

subregistries defined for that registry. Note that for this function, the search for police is "urn:emergency:service:serviceagencylocator.police" and not urn:emergency:service:responder.police. The latter would return the SIP interface for the police department, where the former returns a Service/Agency Locator Record URI.

4.15.3 Service/Agency Locator Search by Name

A search for a service or agency in which the search key is a name is provided by the Service/Agency Locator Search Service. The Service is operated by the ESInet operator. The search function may return one or more Service/Agency Locator URIs, a referral to another Service/Agency Locator Search Service, or an error. The name that is searched comes from the Service Names Registry, Section 10.11, (for a service) or the first "org" element in the serviceAgencyJcard in the Service/Agency Locator Record (for an agency).

HTTP method: GET

Resource name .../LocatorRecordUris

Parameters:

Name	Condition	Description
limit	OPTIONAL	Maximum number of results to return
start	OPTIONAL	First item in the page of results, as an ordinal 1-based integer.
serviceAgencyName	MANDATORY	Name, or part of a name using wildcard notation

A successful return includes a LocatorRecordURIArray consisting of:

Name	Condition	Description
count	MANDATORY	Number of items in the array
totalCount	MANDATORY	Total number of items found
locatorIds	MANDATORY	Array of LocatorRecordUri

LocatorRecordUri consists of:

Name	Condition	Description
uri	MANDATORY	URI of ariLocator Record or another Service/Agency Locator
serviceAgencyName	MANDATORY	Name of Service or Agency whose URI is returned. May occur more than once
uriType	MANDATORY	Either "RecordUri" or "ReferralUri"

© Copyright 2011-2022 National Emergency Number Association, Inc.

Status Codes

200 OK
404 Not Found
454 Unspecified Error

To allow searches beyond the local ESInet, the Search Service is provisioned with other Search Services' URIs much like a Forest Guide.

Note: A future version of this document will specify a more general way to connect the Service/Agency Locator Search Services.

4.15.4 Service/Agency Locator Record

The data returned by dereferencing a service/agency locator record URI is a JSON data structure containing the following elements:

Name	Condition	Use
recordId	MANDATORY	Id of this record at this S/AL
serviceAgencyId	MANDATORY	ServiceId or AgencyId of the Service or Agency
serviceAgencyName	MANDATORY	Official name of Service or Agency
serviceAgencyJcard	MANDATORY	Service operator or Agency Contact information. The name of the service or agency is found in the first 'org' field of the jCard.
serviceAgencyTypes	MANDATORY	Array of Service or Agency Type (psap, police, fire, …)
emergencySipInterfaceUri	CONDITIONAL See Note 1	Interface where 9-1-1 SIP calls are accepted (Note 2)
adminLineUri	CONDITIONAL See Note 3	sip or tel: URI containing 10 digit admin line #, see Section 4.2.1.1.
loggingServiceUriArray	OPTIONAL See Note 4	Service or Agency Logging Service interface, see Section 4.12.1
eidoInterfaceUri	OPTIONAL See Note 5	EIDO Interface URI, See Section 4.12.1
mdsFeatureIntefaceUri	OPTIONAL	MappingDataService Web Feature Service interface
mdsImageIntefaceUri	OPTIONAL	MappingDataService Web Map Service interface
svcStateUri	CONDITIONAL	Service State Subscription URI for a service, such as the PSAP service.
dscRptSvc	OPTIONAL See Note 6	Discrepancy Report Service URI, see Section 3.7

© Copyright 2011-2022 National Emergency Number Association, Inc.

Name	Condition	Use
headJcard	OPTIONAL	jCard of top agency or service operator official
onDutySuperJcard	OPTIONAL	jCard of supervisor on duty now

Note 1: For all URIs, if the service or agency provides SIP service for handling emergency calls, the URI MUST be provided in the record. For example, if the agency accepts emergency calls transferred to it, it MUST provide the emergencySipInterface URI.

Note 2: This URI MUST be provided and MUST be the same URI obtained from the SRV record for the SIP service for the domain of the service or agency. If there is any discrepancy, the SRV record SHOULD be used. This URI is also the same URI obtained directly from the ECRF for the appropriate service URN.

Note 3: Not all agencies will have an admin line that accepts emergency calls. Not relevant for services.

Note 4: Although unusual, not all agencies have a Logging Service.

Note 5: Although unusual, not all agencies have an EIDO interface. Not relevant for services.

Note 6: Although unusual, not all agencies or services have a Discrepancy Reporting Service.

4.15.5 Service/Agency Locator Inter-ESInet Index

A Service/Agency Locator may be aware of other Service/Agency Locators. It can ask those external Locators the names for which it has records, so that it can provide an appropriate referral when it gets a query for a name for which it does not provide records. This index can also contain records for names that the responding Locator has discovered using this mechanism.

The number of agencies listed in a nationwide index could number 100,000-400,000 agencies. As the response to this query can be quite large, "limit" and "start" parameters are available. The server treats all the names it knows (names for which it has records and names it has learned from other Locators) as a single list with the name, the URI of the Locator that has the record (which may be its own URI), and a simple index. which starts at one. The client specifies the maximum number of names it will accept in the response, and the starting index, which is one to retrieve records from the beginning. The response is a series of arrays of names prefaced by the URI of the Locator that has the record for that name. The index of the last name provided is also returned. The client can increment the last index by 1 and use that as the starting index for a subsequent call to the service. A status code is provided for the end of the list. The server MAY supply less than the number of names requested by the client in its response, but it MUST NOT supply more. The server

© Copyright 2011-2022 National Emergency Number Association, Inc.

may restrict this service to other Service/Agency Locators, which would be denoted in the PCA-issued credential.

Discovering other Service/Agency Locators to use this function can be accomplished by provisioning but can be entirely automated by using the Search by Location function in Section 4.15.2. To do so, the Service/Agency Locator itself is a "Service", so the ECRF can be searched for the Service/Agency Locator for a location. In addition, Section 3.4.1 requires the ECRF to return the entire service boundary for the Service/Agency Locator when queried by an entity with a credential traceable to the PCA. A Service/Agency Locator can then create a list of other Service/Agency Locators by querying by location for a Service/Agency Locator, say for a point in the middle of a state, and getting the service boundary of that Locator. It might cover the state, or it might cover a part of the state. If the latter, another search for a point in the state but outside the boundary of the initial Locator will get the URL of another Locator, and it's service boundary, and repeating this will get all the Locators in the state. This sequence can be repeated for all states. This discovery function need only be done perhaps once a year as the boundaries do not change often, and when the name retrieval is executed, the service area of the Locator queried could be verified to see if it is the same as it was when the discovery sequence was completed. It is RECOMMENDED that a state level Service/Agency Locator be created which runs this procedure, and if there is a local or regional Service/Agency Locator, that it refer out of area queries to the state Service/Agency Locator which could provide referrals for any other Locators in the state or in any other state.

HTTP method: GET

Resource name .../NameSets

Parameters:

Name	Condition	Description
limit	OPTIONAL	Maximum number of results to return
start	OPTIONAL	First item in the page of results, as an ordinal 1-based integer.

A successful response returns a NameSetArray

Name	Condition	Description
count	MANDATORY	Number of items in the array
totalCount	MANDATORY	Total number of items found
nameSet	MANDATORY	Array of NameSet

© Copyright 2011-2022 National Emergency Number Association, Inc.

NameSet consists of:

Name	Condition	Description
locatorUri	MANDATORY	URI of Service/Agency Locator
names	MANDATORY	Array of Service/Agency Locator Names

Status Codes

200	OK
404	Not Found
441	Index beyond available names
454	Unspecified Error

4.16 Policy Store

4.16.1 Functional Description

A Policy Store holds policies created by an agency and used by a functional element such as an ESRP. The Policy Store is a simple repository; it does not manipulate the policy.

4.16.2 Interface Description

A Policy Store implements the policy storage and retrieval functions defined in Section 3.3.1. Policy Store replicas can be maintained by having one Policy Store retrieve policies from another Policy Store and subsequently accept requests to retrieve such policies. Replicas normally do not allow a Policy Store operation for a policy that they replicate. There is always one (possibly redundant) authoritative Policy Store for a given policy.

4.16.3 Roles and Responsibilities

Any agency may operate a Policy Store. While it is permissible for an element to contain a Policy Store that it uses, it normally is not authoritative, but rather a replica of the policy. The element must have a mechanism for retrieving the policy from the authoritative source rather than using the internally stored replica, if provisioned to do so.

4.17 Time Server

The ESInet MUST provide an NTP service for time of day information. The service may have a hardware clock, or may be synchronized to another NTP time service provided that there are sufficient backups so that if the ESInet is isolated from its time source, it can provide local time. Time accuracy MUST be within 1 ms of true time. Agencies MAY have their own time server, which MAY have a hardware clock if it is more accurate than syncing the server to the ESInet time server.

© Copyright 2011-2022 National Emergency Number Association, Inc.

4.18 Originating networks and Devices

A device, network, or service provider presenting calls to an ESInet is expected to support the following interfaces. The manner in which the originating network, device, or service arranges its emergency calling services to meet this standard is beyond the scope of this document.

4.18.1 SIP Call Interface

The originating network is expected to present calls to the ESInet meeting the ESInet SIP interface specified in Section 3.1. All calls will be signaled with SIP, MUST contain a Geolocation header field, except if they are calls to an administrative number, and MUST be routed by the ECRF, or an equivalent function that produces the same result, using the location contained in, or referenced by the Geolocation header field.

4.18.2 Location by Reference

Originating networks that are also access networks are expected to also provide a Location Information Server function (i.e., location dereference, and location validation if applicable) meeting the requirements of Section 4.10, if they supply location by reference.

4.18.3 Additional Data Repository

Originating networks and devices presenting calls to ESInets are expected to provide an Additional Data Repository interface meeting the requirements of Section 4.11 unless they always send Additional Data by value.

4.19 Mapping Data Service (MDS)

When answering calls out of area, the answering PSAP needs to be able to display an appropriate map covering the area in which the caller is located, just as if the call was received from an in-area caller. Today, if a call is answered locally, or even in a neighboring PSAP, the data needed to construct a map is available locally. However, if a call was answered in a totally different PSAP, one which does not have a mutual aid agreement, for example, the answering PSAP likely would not have the GIS data from the serving PSAP to construct a map. The Mapping Data Service (MDS) provides this capability. In addition, it is often desirable for all elements within a PSAP that need to display a map to have the same display as other elements which display maps, and differences between implementations of multiple elements are often significant, which makes training and use complicated. The MDS MAY be used by all elements within a PSAP to show consistent displays, but it is not a requirement of this standard that they do so.

All PSAPs MUST have an MDS available to hold their data. The MDS MAY be shared. The MDS MUST be provisioned with GIS data from the layers that are provisioned to the ECRF

© Copyright 2011-2022 National Emergency Number Association, Inc.

as well as layers defined in the NG9-1-1 GIS Data Model [184] that are not included in Appendix B. The service can return a set of GIS features from a specified set of layers within a lat/long bounding box using the Web Feature Service (WFS) [93], or it can return an image file rendered from a similar set of features with a similar input specification plus a "viewport"[50] specified by the number of pixels in X and Y using the Web Map Service (WMS) [186]. The MDS supports both interfaces, and clients may choose which one to use. Note that if the WFS interface is used, the client receives a set of features and it determines what the map looks like. If WMS is used, the MDS determines what the map looks like.

The querier may specify which layers it wishes to receive in the return feature set or image. For this purpose, a registry listing every layer that could be supported by the MDS is defined in Section 10.32. A given GIS system may not have every layer defined in the registry and thus the return feature set or images may be a subset of the layers requested.

The MDS for a given location is discovered with the Service Locator function. It is queried with one of two Web Service interfaces: a Web Feature Service (WFS) interface for features and Web Map Service (WMS) for images as defined below.

The MDS MUST offer a Web Feature Service Version 2.0.2 [93]. The WFS MAY support:

- Insert, Update, or Delete operations
- Transaction/lock capability
- Stored queries
- Filters (other than BBOX)

The WFS MUST support GML 3 output format. Other formats MAY be supported.

The MDS MUST offer a Web Map Service Version 1.3.0 [186]. The WMS MUST support the EPSG:4326 Coordinate Reference System (CRS) [187] and MAY support others for each layer it provides. The WMS MUST support a PNG output file format and MAY support others. The WMS MUST support at least 15 layers and MaxWidth and MaxHeight of at least 2048. The WMS must be capable of supporting every layer defined by the NENA Standard for GIS Data Model, NENA-STA-006.1-2018 [184], although the WMS may not be provisioned for every layer in every area it supports and thus MAY not be able to respond to a request for a layer for which it has no data. It MAY support other layers. The layer name MUST be the layer name as defined in the NENA Standard for NG9-1-1 GIS Data Model [184].

[50] The visible area on a screen where an image is rendered. Usually specified as the X and Y pixel location of two opposite corners, or the X and Y pixel location of one corner and a height and width, the viewport is the destination of a rendering operation such as rendering a part of a map onto a display.

© Copyright 2011-2022 National Emergency Number Association, Inc.

To maintain a local copy of the MDS, the PSAP could obtain the SI feed to its data. It could also obtain SI feeds from the data provider of any neighboring MDS.

No common style definition is provided in this edition. A future edition may provide a common style definition to improve uniform display of WMS data.

4.20 Outbound Call Interface Function (OCIF)

The Outbound Call Interface Function is part of the NGCS and responsible for handling calls originating from i3-PSAPs over their serving ESInet/NGCS. The OCIF is used to process callbacks as well as other outgoing calls that transit the ESInet (e.g., official calls from one Public Safety agency to another, perhaps on a different ESInet), including admin calls promoted to emergency calls. The OCIF is on the border of the ESInet. It allows traffic outbound to another PSAP hosted on the same ESInet. It also allows traffic outbound from the serving ESInet to interconnected networks[51]. The OCIF MUST NOT allow any calls or other SIP operations inbound from any source to entities inside the ESInet. An OCIF MAY include a Session Border Controller as part of its functionality.

The OCIF operates as a SIP proxy server (or B2BUA in some circumstances), routing callbacks to an interconnected network, which will ultimately forward the call toward the caller's device, possibly via one or more other networks. The NGCS provider MUST have an IP-based Network-to-Network Interface (IP-NNI) with one or more interconnected network providers to facilitate callbacks routed via the OCIF. Note that other outgoing calls initiated by a PSAP, such as those destined for another agency, may also transit the ESInet. Such calls will also be processed by the OCIF. In addition, outbound ESInet calls destined to the PSTN MUST go through the OCIF, which will interwork SIP to SS7 through a standard PSTN Gateway[52]. Alternatively, OCIF PSTN access COULD be provided by an interconnected network provider. In such case, the SIP to SS7 interworking will be provided by the interconnected network provider.

The OCIF MUST support all media types listed in this standard. All callbacks MUST be marked with the value "psap-callback" in the Priority header field as documented in RFC 7090 [141].

---

[51] Interconnected networks include directly connected originating networks, transit networks, and other ESInets.

[52] Technical details of the PSTN Gateway function and its legacy interface to the PSTN are outside the scope of this document.

© Copyright 2011-2022 National Emergency Number Association, Inc.

The ESRP MAY be used to route callbacks and other outgoing calls from a PSAP toward the OCIF. If included in the call path, the ESRP SHALL route the outgoing call to the OCIF. The OCIF SHALL forward the call to the appropriate interconnected network.

SIP INVITE messages for callbacks destined to be routed through an OCIF MUST contain:

1. A Request-URI line containing the callback URI;
2. A To header field populated with the callback URI. Usually the value is the content of the P-A-I (preferred, if present) or From header field of the original emergency call;

Note: The callback URI MUST contain a dialable telephone number either expressed as a national 10-digit NANP number or as an international number following ITU-T Recommendation E.164 and, if expressed as a sip URI, the domain part SHALL represent the home network of the target. If the original emergency call was from a non-service initialized handset, the callback number of the form "911 plus the last 7 digits of the ESN or IMEI expressed as a decimal" is not dialable and therefore MUST NOT be used for callback.

3. A From header field containing sip:TN@<psapdomain>;user=phone, which SHOULD be the same value as in the P-A-I header field;

Note: The OCIF MUST support receipt of outgoing calls from PSAPs marked for presentation restriction of caller ID expressed by the presence of a Privacy header field (RFC 3323 [207], expanded by RFC 3325 [16] and RFC 7044 [35]) and the From header field value populated with "Anonymous" sip:anonymous@anonymous.invalid;

4. A Route header field populated with a routing URI that should contain the "lr" parameter to avoid Request-URI rewriting (the INVITE from the PSAP MAY contain the outgoing ESRP, or, if ESRPs are not used to route callbacks in the ESInet originating the callback, the OCIF URI. An INVITE from an ESRP to the OCIF SHALL contain the OCIF URI. The INVITE from the OCIF to the interconnected network SHALL contain the well-known URI associated with that network);
5. A SIP Priority header field with "psap-callback" as the value;
6. A Resource-Priority header field with "esnet.0" as the value;
7. A P-Asserted-Identity header field containing sip:TN@<psapdomain>;user=phone, where the TN is associated with the PSAP originating the call, and can be asserted by an Secure Telephone Identity Authentication Service (STI-AS) function;
8. A second P-Asserted-Identity header field containing the identity of the agent originating the call expressed as sip: "agent name" <agentID@agencyID>;

Note: The Display Name part is OPTIONAL;

© Copyright 2011-2022 National Emergency Number Association, Inc.

9. An SDP offer containing all media supported at the PSAP. The SDP SHOULD include offers matching the negotiated SDP from the original emergency call, placing the SDP that was used as the top-most value in the list;

The OCIF processing a callback INVITE constructed as above will interact with the STI-AS FE to assert the telephone identity of the caller. Once the assertion and signing process is completed, the OCIF will receive the INVITE back with an added SIP Identity header field constructed per RFC 8224 [60], using the NGCS provider's credentials as the signing authority for the PSAP telephone identity.

Note: The INVITE message received back from the STI-AS MUST be constructed in such a way that the OCIF will recognize it as a "spiral" as defined in RFC 3261 [10], if the OCIF has loop detection enabled.

SIP INVITE messages for other outgoing calls that transit the ESInet through an OCIF MUST contain:

1. A Request-URI line containing the target URI;
2. A To header field populated with the target URI, as determined by the initiating PSAP;

Note: The target URI MUST contain a dialable telephone number either expressed as a national 10-digit NANP number or as an international number following ITU-T Recommendation E.164, or a sip URI that is routable within the ESInet, where the domain part represents the home network of the target.

3. A From header field containing sip:TN@<psapdomain>;user=phone, which SHOULD be the same as in the P-A-I header field;

Note: The OCIF MUST support receipt of outgoing calls from i3-PSAPs marked for presentation restriction of caller ID, expressed by the presence of a Privacy header field (RFC 3323 [207], expanded by RFC 3325 [16] and RFC 7044 [35]) and the From header field value populated with "Anonymous" sip:anonymous@anonymous.invalid;

4. A Route header field populated with a routing URI that should contain the "lr" parameter to avoid Request-URI rewriting (the INVITE from the PSAP MUST contain the outgoing ESRP. The INVITE from the ESRP to the OCIF SHALL contain the OCIF URI. If the INVITE from the OCIF is to an interconnected network, it MAY contain the well-known URI associated with that network);
5. A Resource-Priority header field populated with an appropriate value based on section 3.1.7 (e.g., "esnet.0" or "esnet.2") as determined by the originating PSAP;

© Copyright 2011-2022 National Emergency Number Association, Inc.

6. A P-Asserted-Identity header field containing sip:TN@<psapdomain>;user=phone, where the TN is associated with the PSAP originating the call and can be asserted by an STI-AS function;
7. A second P-Asserted-Identity header field containing the identity of the agent originating the call expressed as sip:"agent name"<agentID@agencyID>;

Note: the Display Name part is OPTIONAL

8. An SDP offer containing all media supported at the PSAP;

The OCIF processing an outgoing INVITE constructed as above will interact with the STI-AS FE to assert the telephone identity of the caller. Once the assertion and signing process is completed, the OCIF will receive the INVITE back with an added SIP Identity header field constructed per RFC 8224 [60], using the NGCS provider's credentials as the signing authority for the PSAP telephone identity.

Note: The INVITE message received back from the STI-AS MUST be constructed in such a way that the OCIF will recognize it as a "spiral" as defined in RFC 3261 [10], if the OCIF has loop detection enabled.

The OCIF service interfaces are SIP/RTP based and MUST conform to sections 3.1 and 3.1.9. The generic SIP interface from the OCIF to an interconnected network MUST conform to the definition of the SIP interface as defined in Section 3.1, except:

1. The Request-URI line MUST NOT contain an "sos" service URN;
2. The Geolocation and Geolocation-Routing header fields MUST NOT be used;
3. The P-Asserted-Identity header field MUST be present and populated with a value that can be asserted through an STI-AS function;
4. P-type headers other than P-A-I are OPTIONAL;
5. No purpose for the Call-Info header field is yet defined;
6. Header fields listed in Section 3.1.6 MAY be used.

The OCIF MAY, based on local policy, add a P-Charge-Info header field (RFC 8496 [208]) and/or a P-Charging-Vector header field (RFC 7315 [209]) on the outgoing INVITE.

The OCIF has a SIP interface to the STI-AS FE (see section 4.21.3) for the purpose of asserting and digitally signing the telephone identity (i.e., the telephone number) of PSAP-originated outbound calls. The OCIF invokes the STI-AS FE for any call presented to it after call processing has completed, that is, after the destination interconnected network has been determined.

4.21 Secure Telephone Identity (STI)

The Secure Telephone Identity (STI) Authentication Service is an NGCS functional element that provides caller identity assertion for callbacks and other PSAP-originated outbound

© Copyright 2011-2022 National Emergency Number Association, Inc.

calls. The STI Verification Service is an NGCS functional element that provides verification services applicable to emergency calls destined for i3 PSAPs. Both the Secure Telephone Identity Authentication Service (STI-AS) and the Secure Telephone Identity Verification Service (STI-VS) FEs are defined by the SHAKEN framework as specified in ATIS-1000074-E (errata) [210]. The STI-AS and STI-VS FEs adhere to ATIS-1000074-E (errata) unless otherwise specified herein.

The SHAKEN reference architecture specified in ATIS-1000074-E (errata) also includes the Call Validation Treatment (CVT) and Secure Key Store (SKS) elements.

For emergency calls, the STI-VS FE provides the results of the verification process to downstream entities to help detect potential telephone scams using spoofed telephone numbers such as SWATting, prank calls and illegitimate robocalling. For PSAP-originated outbound calls, including callbacks, the STI-AS FE asserts and cryptographically signs the telephone identity of the caller, allowing PSAP-originated calls to be validated by the networks these calls transit through (if they support such capabilities), and for the home network performing the verification to present the called party with an indication of the validity of the calling telephone number (if it supports such capabilities). Calls with a validated telephone identity have a higher chance of completing at the called party, which is an important feature for emergency callbacks.

© Copyright 2011-2022 National Emergency Number Association, Inc.

The STI-AS and STI-VS FEs interconnect with NGCS as per the following diagram.

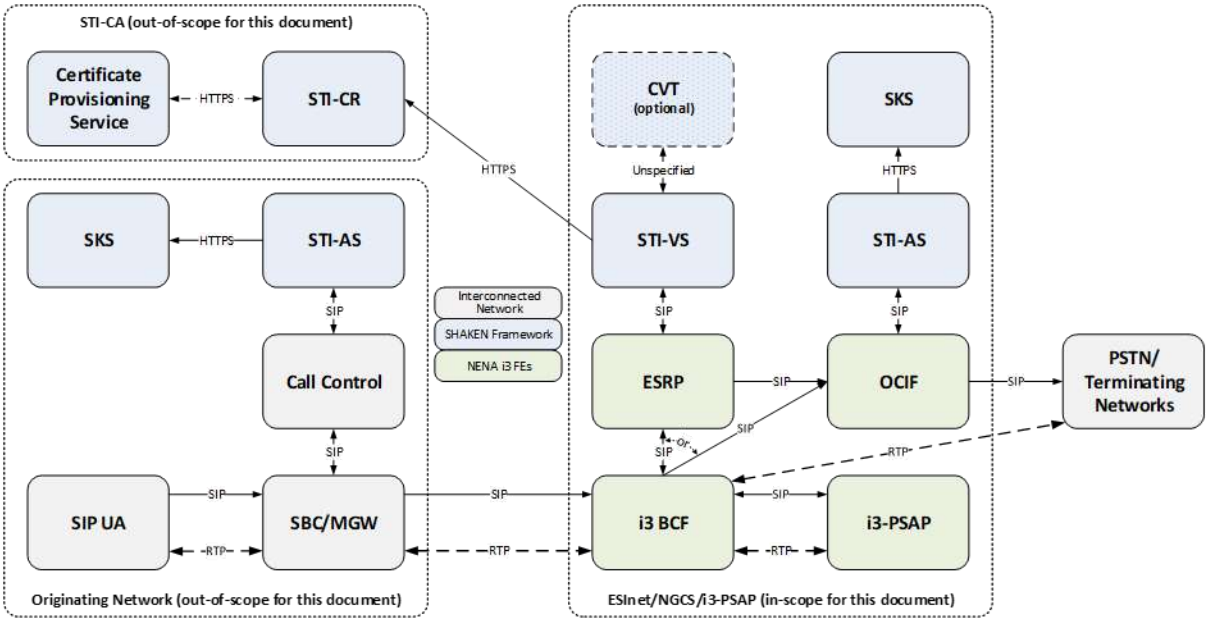


Figure 21 - NGCS-STI Interconnection Architecture

The STI-VS FE supports caller identity validation for emergency 9-1-1 calls presented to the ESInet/NGCS (forward path) and the STI-AS FE supports i3 PSAP-originated caller identity assertion for outbound calls transiting through the ESInet/NGCS (reverse path), such as emergency callback calls. The STI-VS FE interacts with the ESRP for inbound emergency calls and the STI-AS FE interacts with the OCIF for outbound calls originated from i3-PSAPs and transiting the ESInet.

Note: This document does not impose any requirements on Originating Networks to support STIR and SHAKEN. It defines the procedures an NGCS SHALL apply to 9-1-1 emergency calls that are presented with SHAKEN-compliant signaling in order to provide caller identity verification services to i3 PSAPs, as well as caller identity assertion services for calls originating from i3 PSAPs over the ESInet/NGCS and presented to interconnected networks for verification, if supported by such networks.

The STI-VS FE and the STI-AS FE MUST implement a logging interface as per Section 4.12.

Note: All transactions and every message sent and received via the service interfaces MUST be sent to the Logging Service.

Each STI server MUST implement the server-side of the ElementState event notification package, including its sub-components.

© Copyright 2011-2022 National Emergency Number Association, Inc.

The STI-VS FE and the STI-AS FE MUST implement the server-side of the ServiceState event notification package, including its sub-components.

Note: The concept of Secure Telephone Identity is nascent. As such, it is expected that the referenced standards will evolve. A future version of this document will ensure alignment with the evolution of these standards, when appropriate.

4.21.1 STI Verification for Emergency 9-1-1 Calls

The STI-VS FE is invoked by the ESRP before call processing has completed; that is, before applying Origination Policies.

For emergency 9-1-1 calls presented to the ESInet/NGCS with an Identity header field populated as per RFC 8224 [60], the procedures defined in ATIS-1000074-E (errata) for the STI-VS SHALL be applied with the following clarifications.

- If the To header received by the STI-VS in the incoming INVITE message contains a URI that can be interpreted as "911" or an sos service urn (e.g., urn:service:sos), the content of the To header in the received INVITE does not match the "dest" claim in the PASSporT, and the "dest" claim in the PASSporT is something other than a URI that can be interpreted as "911" or an sos service URN, the "dest" claim verification SHALL be considered failed;
- If the To header received by the STI-VS in the incoming INVITE message contains a URI that can be interpreted as "911" or an sos service urn (e.g., urn:service:sos), the content of the To header in the received INVITE does not match the "dest" claim in the PASSporT, and the "dest" claim in the PASSporT contains a URI that can be interpreted as "911" or an sos service URN, the "dest" claim verification SHALL be considered passed;
- If the Request-URI and the To header field contain a URI that can be interpreted to be "911", the "dest" claim verification procedure SHALL be considered passed if a match is found;
- If the Request-URI is a service URN (e.g., urn:service:sos)[53] and the To header field contains a URI that can be interpreted to be "911", the "dest" claim verification procedure SHALL be considered passed;
- If the Request-URI and the To header field value contain a service URN (e.g., urn:service:sos)[54], the "dest" claim verification procedure SHALL be performed and considered passed if a match is found;

[53] Additional work outside of NENA is in progress to support this scenario

[54] Additional work outside of NENA is in progress to support this scenario

© Copyright 2011-2022 National Emergency Number Association, Inc.

- Emergency 9-1-1 calls MUST always be progressed forward regardless of the success or failure of the verification process. If the verification process fails, the STI-VS FE MUST include the error response code and a reason phrase in a Reason header (RFC 3326 [18]) field added to the next response (provisional or final) back to the Originating Network. The STI-VS FE MAY issue a Discrepancy Report to the Originating Network as per section 3.7.14;
- Emergency calls that include a Resource-Priority header field populated with a value from the "esnet" namespace SHOULD be passed to the CVT[55], if this component is available from the NGCS provider.

Upon having completed its verification steps, the STI-VS SHOULD invoke the CVT, if available. The processing performed by the CVT and the interface used to convey the results of that processing are left to implementations.

For the calling number, the STI-VS FE MUST add the "verstat" parameter to the P-Asserted-Identity header field or From header field to convey the results of the verification and forwards the call to the ESRP on the same queue the call originally arrived on. The ESRP then processes the call as per its normal procedures i.e., applying Origination Policies, ECRF query, etc.

4.21.2 STI Authentication for PSAP-Originated Calls.

The STI-AS FE is invoked by the OCIF after call processing has completed, that is, after the interconnected network has been determined.

The STI-AS functions as described in ATIS-1000074-E (errata) [210], and the output is a cryptographically signed Personal Assertion Token (PASSporT) as defined in RFC 8225 [203], inserted in an Identity header field as per RFC 8224 [60] in the outgoing SIP INVITE message.

4.21.3 Call Validation Treatment

The Call Validation Treatment (CVT) is an optional, value-add FE providing call spam analytics and possibly other mitigation techniques. It interacts with the STI-VS and returns a response that influences what should be signaled to the called party for a legitimate or illegitimate call.

ATIS-1000074-E (errata) [210] provides a high-level view of the CVT FE. However, its interfaces and detailed specifications are purposely not defined and left to the vendor community to specify. It is included here for alignment with the ATIS standard.

---

[55] Additional work outside of NENA is in progress to support this scenario.

© Copyright 2011-2022 National Emergency Number Association, Inc.

4.21.4 STI Secure Key Store

The STI Secure Key Store (STI-SKS) FE provides a highly secure storage for private keys to be used for cryptographically signing SIP INVITE messages presented to the STI-AS FE. It interacts with, or is part of, the STI-AS FE.

ATIS-1000074-E (errata) [210] provides a high-level view of the STI-SKS FE, with further details related to the management of STI certificate/key management provided in ATIS-1000080-E [211]. The NGCS STI-SKS SHALL store keys in a FIPS-PUB-140-3 [67] level 3 or higher key store. Certificates for signing keys SHALL be signed directly by the root key.

Note: It is an objective that the NGCS' root signing keys will be traceable to the PCA, and the PCA's certificate will be cross signed by the ATIS STI Certificate Authority.

4.22 Incident Data eXchange (IDX)

The Incident Data eXchange (IDX) functional element collects Emergency Incident Data Objects (EIDOs). The IDX receives requests for EIDOs and puts the information together. A detailed description of IDX functionality/interfaces will be part of a future version of this document.

5 Security

This section contains information about specific considerations for this Standard. For other security considerations, see NENA 75-001 [231].

5.1 Identity

Each agency and each agent in an agency are issued credentials that allow them to be identified to all services in the ESInet. An agency identifier is a globally unique FQDN (such as "erie.psap.ny.us"), which appears in the SubjectAltName of an X.509 [144] certificate issued to the agency. The agency assigns identities to an agent. The identity for an agent is a string containing a userpart which is unique to the agent within the agency, an "@", and the FQDN of the agency. For example: "nancy@erie.psap.ny.us". This string appears in the SubjectAltName of an X.509 certificate issued to the agent. See Identifiers in Section 2.1.

For PSAPs and 9-1-1 Authorities, the root Certificate Authority for agent and agency certificates is the PSAP Credentialing Agency (PCA). The certificate can be issued directly by the PCA, or the PCA can issue a certificate to an agency that, in turn, issues certificates to other agencies or agents. It is recommended that a state PCA be created for each state, with the national PCA signing the state PCA certificate, and the state PCA signing 9-1-1 Authority and PSAP certificates. 9-1-1 Authorities or PSAPs may sign the certificate of their agents.

© Copyright 2011-2022 National Emergency Number Association, Inc.

Operating a CA requires the creation of, and strict adherence to, a Certificate Policy and Practice Statement (CP/CPS) [59]. A CP/CPS includes strict specifications for vetting: who gets a certificate, under what conditions they get a certificate, and what proof of identity is needed before a certificate can be issued. If an agency cannot reasonably control its certificate issuing mechanisms it SHOULD contract to an entity that can provide strong controls and strict adherence to a suitable CP/CPS. NENA foresees that other agencies such as police, fire, and EMS agencies will need a similar Public Key Infrastructure (PKI), and it may be that, for example, a county level agency provides the Certificate Authority for all agents in the county.

Great care MUST be taken to protect private keys. Key storage options are defined in FIPS-140-2 [67] agency keys MUST be protected with at least LEVEL 2, and LEVEL 3 is highly recommended. CA keys for agency CAs MUST meet LEVEL 3 requirements. State and National CA keys MUST be stored in a LEVEL 4 device.

The identities, and the credentials, MUST be presented to gain access to ALL services and data in the ESInet.

5.2 PSAP Credentialing Agency

The PCA CP/CPS MUST be in conformance with the minimum standards included in this document. Any agency or agent may obtain a certificate from the PCA through the appropriate CA for that jurisdiction. Prior to the PCA being available in a given jurisdiction, NG9-1-1 implementations SHOULD accept credentials issued by any certificate authority listed in the current Mozilla Certificate Store (https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/).

5.3 Roles

When authenticating within the ESInet, an agent or agency assumes one or more roles. The roles which an agent or agency may assume are limited by policy of the immediately superior agency. The Role is contained in the X.509 certificate of the agency or agent.

Agency Roles defined within this specification are:

- PSAP per NENA ADM-000 Master Glossary: "… responsible for receiving 9-1-1 calls and processing those calls according to a specific operational policy."
- Dispatch per ANS1.107.1.2015 "… alerting and directing the response of public safety responders to the desired location".
- 9-1-1 Authority – per NENA ADM-000 Master Glossary: "… governmental entity responsible for 9-1-1 service operations.
- ESInet Service Provider – The entity responsible for the operation of an Emergency Services IP Network.

© Copyright 2011-2022 National Emergency Number Association, Inc.

- ESRP Service Provider – The entity responsible for the operation of an Emergency Service Routing Proxy
- ECRF/LVF Service Provider – The entity responsible for the operation of an Emergency Call Routing Function/Location Validation Function.
- LIS Service Provider – The entity responsible for the operation of a Location Information Server.
- Any responder agency listed in the "urn:emergency:service:responder" Registry (see Section 10.5).
- Agency Role modifier are scopes that can be applied to the above agency roles to further clarify the extent of the authority:
    - National
    - State
    - Regional
    - Local

A registry for Agency Roles is defined. See Section 10.27. While ESInet implementations may define other roles for agencies, it is RECOMMENDED that the policies of the ESInet provide 100% functionality without additional roles so that availability of resources is maximized when disaster situations occur and other ESInets and agencies are providing services to the PSAPs. In the same vein, all ESInets MUST have agencies that assume all of the above roles.

Agent Roles defined in this specification are:

- Dispatching Role – per ANS1.107.1.2015 "… alerting and directing the response of public safety responders to the desired location".
- Call Taking Role – per ANS1.107.1.2015 "… processes incoming calls through the analyzing, prioritizing, and disseminating of information to aid in the safety of the public and responders".
- GIS Analysis Role – assembles and maintains geospatial and addressing information.
- IP Network Administration Role – monitors, manages, and controls network elements and services (e.g., switches, routers, gateways, firewalls, and network services such as DNS and DHCP); plans for and responds to service outages and other problems.
- Database Administration Role – installs, configures, manages, monitors, and controls access to databases.
- IT Systems Administration Role – installs, configures, supports, and maintains system hardware, operating systems, application elements and services; plans for and responds to service outages and other problems.
- Application Administration Role – installs, configures, supports, and maintains applications; plans for and responds to service outages and other problems.

© Copyright 2011-2022 National Emergency Number Association, Inc.

- Security Administration Role – creates, assigns, configures, maintains, and supports user authentication and authorization elements and services; monitors for possible security violations and vulnerabilities, and ensures that vulnerabilities are corrected.
- Records Production Role – searches for, retrieves, and reproduces records and recordings for internal and external uses, including FOIA requests, subpoenas, and media requests.
- Data Analysis Role – researches and analyzes specific kinds of data to identify trends, anomalies, and conditions important to supporting emergency services.
- Quality Assurance Evaluation Role – per ANS1.107.1.2015 "… reviews telecommunicator work performance and documents an evaluation of the level of compliance with Agency directives and standards".

Role Modifiers (may be added to further specify the above roles):

- Management Role
- Supervision Role
- Trainer Role
- Trainee Role
- Assistant Manager
- Shift Supervisor (to include Dispatch, Call Taking or a combination of both
- Dispatcher
- Call taker
- GIS Specialist
- GIS Supervisor
- Maintenance Supervisor
- Maintenance Technician
- Temporary Technician
- ESInet Network Operator
- ESInet Network Operations Supervisor
- 9-1-1 Authority Director
- 9-1-1 Authority Agent
- Database Administrator
- IT Systems Analyst
- Records Production Specialist

Specific definitions of these roles will be provided in a NENA Information Document to be referenced in a future version of this document. A registry of Agent Roles is defined. See Section 10.28.

© Copyright 2011-2022 National Emergency Number Association, Inc.

5.4 Authentication

Authentication of Agents accessing elements described in this document MUST be implemented with a universal Single Sign On (SSO) paradigm. The mechanism used is OASIS SAML (Security Assertion Markup Language). There are two entities: an Identity Provider (IDP) which authenticates users and supplies the other parry with a "token" that can be used in subsequent operations to refer to an authorized user, and a Relying party which uses the token. SAML is used by a Relying Party to ask if a user should be permitted to perform an operation. Agents in PSAPs and Responder Agencies, as well as other service agencies with agents use the SSO mechanism for all operations requiring agent authorization. In this document, the only mechanism defined that uses these tokens is the Authorization and Data Rights Management mechanism, but any application or service that uses Agents SHOULD use this mechanism for any authentication and authorization decisions for Agents. For establishment of TLS sessions between agents and elements, the SSO mechanism is used to authenticate the agent, which is then used to unlock the private key for that agent, and the key is used (together with its accompanying X.509 certificate) to establish the TLS session.

For applications that depend upon interactions with Agents, several profiles of the Security Assertion Markup Language Version 2 [58] as amended by errata shall be used. SAMLv2, is an XML-based framework for describing and exchanging security information.

SAMLv2 consists of a suite of core specifications, which outline schema and protocols [58], transport bindings [127], and a set of concrete profiles [128], which carefully orchestrate bindings and message patterns for SAML processors to discover SAML authorities and relying parties, as well as to request, produce, send, and receive SAML assertions. Also specified are the publication and discovery mechanisms for entity metadata [129] necessary for bootstrapping interactions between parties.

For HTTP-bound NG9-1-1 web applications, the following existing SAMLv2 profiles MUST be supported by both asserting parties (i.e., IDP) and relying parties (i.e., RP), as specified in [128]:

- Web Browser SSO Profile
- Identity Provider Discovery Profile
- Single Logout Profile.

In addition, the following profiles MAY be supported:

- Enhanced Client or Proxy (ECP) Profile
- Artifact Resolution Profile.

The Web Browser SSO Profile outlines the exchanges for requesting and producing SAMLv2 assertions, in the presence of a web browser-based user-agent, which is used as the

© Copyright 2011-2022 National Emergency Number Association, Inc.

intermediary transport agent for these request, via orchestrated HTTP 302 redirects. For systems that use a client application to authenticate a user, the X500 profile of [128] is used.

The Identity Provider Discovery Profile provides a mechanism for enabling the discovery of authentication authorities by means of a shared HTTP cookie, which carries an enumeration of IDPs to which the client is capable of authenticating. It is RECOMMENDED that this be the primary means for IDP discovery for an actor. Providers are identified by a URI as defined above.

Most SIP and HTTPS sessions covered by this document are server to server. Some involve a client which is an agent (and thus not a server), but all agents, agencies and elements have credentials with certificates traceable to the PCA which can be used with mutual authentication methods. Mutual Authentication MUST be used for TLS and SIP session establishment using a certificate traceable to the PCA.

Note: The mechanism used to implement the SSO requirement may change in version 4 of this document. OpenID is under consideration as a mechanism.

5.5 Trusting Asserting and Relying parties

In order for entities within the NENA infrastructure to be strongly identified in this federated authentication architecture, and for the proper run-time provisioning of new entities within the infrastructure, SAML metadata XML instances, as defined by [129], of each entity SHOULD be aggregated into a single XML instance using the <EntitiesDescriptor> container. This aggregated metadata document MUST be signed (via XML Signature) by an identified administrative body, using a well-known signing certificate. Thus, any entity (and the encryption and signing keys) contained within the <EntityDescriptor> element is identified as an authorized party to the infrastructure.

Within this framework, each identity provider MUST insist on two-factor authentication of agents. The factors defined are:

- Passwords, which must conform to local password policy;
- Tokens (RSA SecurID);
- Smart Cards conforming to ISO/IEC-7816 (1-15) [157];
- Biometrics, including fingerprints, palm prints, retina scans, facial recognition, and voice recognition.

It is RECOMMENDED that all authentication services enroll agents with as many factors as practical and allow any specific authentication to use any two. At present, there are no widely accepted standards for biometric information. Consequently, biometric authentication would only work when the authentication server and enrollment server use the same brand of scanner. Furthermore, if network access to the authentication data is

© Copyright 2011-2022 National Emergency Number Association, Inc.

lost, biometric authentication may not work. All agencies SHOULD have backup mechanisms (such as smart cards) available for local authentication when network access is unavailable.

Protocol operations use RSA-2048 (see RFC 8017 [158]) with the credentials rooted in the PCA, typically over TLS. All elements in the ESInet MUST accept RSA-2048 with a certificate rooted in the PCA. They MAY accept alternate authentication cryptosystems as long as they are at least as strong as RSA-2048. RSA-2048 MUST be supported by all implementations.

All protocol exchanges across the ESInet SHOULD be authenticated.

5.6 Authorization and Data Rights Management

Authorization and Data Rights Management in NG9-1-1 is based on XACML 2.0 [61]. Each XACML policy defines a "target", which describes what the policy applies to (by referring to attributes of users, roles, operations, objects, dates, and more), and one or more "rules" to permit or deny access. Access is defined to mean some combination of:

- Read – the ability to retrieve a data object
- Update – the ability to modify an existing data object
- Create – the ability to create a new data object
- Delete – the ability to remove an existing data object
- Execute – the ability to execute one or more functions from a service

Rules may "permit" or "deny" access.

XACML policies are stored in a Policy Store. The XACML "Policy Decision Point" can be inside the element or agency that has the "Policy Enforcement Point" or may be external to it. Policies have names. The names come from a registry (10.14) or from the Service Names Registry (10.11).

Provisioning data is owned by the agency operating an element, or the agency contracting with the agency operating the element, and thus is subject to data rights management.

In policy rules:

- Subject attributes can include the id (as an agentId), agency (as an agencyId), role (from the Agent or Agency role registries, Sections 10.27 and 10.28), and agencyType (from the agency locator record). The attributes agencyId, agency, role, and agencyType are string types.
- Resources can be data structures or interfaces. Interfaces are named by the element Id and an interface keyword from a registry defined in Section 10.30 separated by an ampersand. Data items are named by the json object name from the OpenAPI interface description that defines them and the element tag (if access is controlled by element) separated by a period. For example, "LoST@ecrf.state.pa.us" and

© Copyright 2011-2022 National Emergency Number Association, Inc.

"civicAddr.A3". If no element name is specified, the access to the entire data structure is controlled by the rule.
- Actions are "Read", "Create", "Update", "Delete", and "Execute".
- A default rule must be included in every policy rule set.

The XACML document is a JWS [171] (see Section 5.10) that MUST be signed by the owner of the Policy and MUST include the certificate and signing chain by value or by reference.

Note: Occasionally data becomes orphaned and must come under new ownership to provide updates. A mechanism to re-home orphaned data will be provided in a future version of this document.

5.7 Integrity Protection

All protocol operations MUST be integrity-protected with TLS, using SHA-256 [62] or stronger. SHA-256 MUST be supported by all implementations. See [213] for details related to SRTP support for SHA-256.

5.8 Privacy

All protocol operations MUST be privacy protected via TLS, preferably using Advanced Encryption Standard (AES) [63] with a minimum key length of 256 bits (AES-256). Shorter key length MUST NOT be used. Systems currently using Data Encryption Standard (DES) or triple-DES MUST be upgraded to at least AES-256. Alternate encryption algorithms are acceptable as long as they are at least as strong as AES.

Stored data which contains confidential information MUST be stored encrypted, using AES-256 or an equivalently strong algorithm. Access to encryption keys MUST be defined by a management policy that is strictly adhered to. Keys MUST NOT be stored in clear text. Access to keys MUST be secured by at least a pass phrase, and a two-factor authentication system for key access is RECOMMENDED. Guidelines for implementing and maintaining stored data securely can be found in [110]. Alternate privacy protection algorithms are acceptable as long as they are at least as strong as AES as long as both sides can implement it. AES-256 MUST be supported by all implementations.

5.9 Algorithm Upgrades

Cryptology choices are constantly being re-evaluated due to ongoing threat analysis, algorithm weakness research and other factors. Implementers should be aware that the mandatory algorithm choices (RSA-1024, SHA-256, and AES-256) to be supported in all implementations as described in this section may need to be upgraded as new threats emerge. At present, only a future version of this document could change the mandatory algorithm requirements.

© Copyright 2011-2022 National Emergency Number Association, Inc.

5.10 JSON Web Signatures

This document, and i3 in general, extensively uses JSON objects. These JSON objects often contain information that needs to be protected against alteration and repudiation. As specified in various parts of this document, the JSON Web Signature (JWS) [171] mechanism is used to provide this protection. Within this document, a JWS MUST use the Flat JSON serialization format (not JWS Compact Serialization and not General JWS JSON Serialization Syntax), and only the Edwards-curve Digital Signature Algorithm (ECDSA) with Curve448 (algorithm "EdDSA") [227] [228] signature method is used.

Each Web Service that has entrypoints in which a JWS is used MUST include the "requiredAlgorithms" parameter in the "serviceInfo" parameter of the object returned by its Versions entrypoint. The "requiredAlgorithms" parameter specifies the JWS signing algorithms [221] permitted by the Web Service's currently in force policy. Implementations MUST support (be capable of generating and using) algorithm "EdDSA" and MUST NOT use other algorithms except that implementations of the Logging Service and clients of the Logging Service MUST support (be capable of generating and using) unsigned (algorithm "none"). A Logging Service MAY include "none"; a policy store MUST NOT include "none". If a Web Service request receives an "Unacceptable Algorithm" error, the client MUST make a new request on the Versions entry point and retry the request with a JWS that uses a signing algorithm acceptable to the Web Service.

Note: Use of other algorithms, especially in situations where third parties may verify a signature, will be considered in a future version of this document.

LogEvents are allowed to be unsigned because of their high volume and the potential for performance impacts; the policy currently in force of the agency operating the Logging Service determines if LogEvents are to be signed or unsigned. For signed LogEvents, the policy in force at the entity creating the LogEvent chooses between the size burden of each LogEvent containing the X.509 certificate of the signer (with all intermediate certificates) versus the additional network transactions the Logging Service or entity accessing the LogEvents needs to perform to retrieve the certificate (and chain) by reference, as described below. (Although this choice potentially impacts the Logging Service, the choice is up to the policy of the agency operating the entity creating the LogEvent).

Implementations that access JWSs MUST support certificates (and chains) both by reference and by value; implementations that generate JWSs MAY use either.

When this document indicates that a set of Web Service interface parameters is a JWS (e.g., for LogEvents), the set of parameters is conveyed in the web service request as a string consisting of a JWS. The JWS is formed by applying the JWS algorithm to the set of parameters per the JWS standard [171].

© Copyright 2011-2022 National Emergency Number Association, Inc.

- The JWS Protected Header MUST contain exactly one "alg" field. The "alg" field MUST have a value acceptable to the Web Service.
- An unsigned (unprotected) JWS is indicated by an "alg" field set to the value "none".
- For signed LogEvents, and all other uses of JWS requiring signatures (e.g., policy documents), the JWS Protected Header MUST have its "alg" field set to a value acceptable to the Web Service that MUST NOT be "none" and MUST specify the signing entity's X.509 certificate and all intermediate certificates up to one signed by the trusted root[56]. The certificate is provided either by reference or by value. A certificate provided by value is contained in an "x5c" field. A certificate is provided by reference using the "x5u" and "x5t#256" fields. When the "x5u" field is present, it MUST contain a URL that is stable (resolvable) for a minimum of 10 years. The JWS Protected Header MAY contain other fields.

Including a certificate (with chain) in each LogEvent increases the size of the event (in some cases by a multiple of the event size) but avoids the additional network requests necessary to retrieve the certificate chain using the "x5u" field.

When the "x5u" field is used, the "x5t#256" field MUST also be used, to allow an entity to more easily detect when a certificate chain needs to be retrieved.

The JWS is passed as the actual parameter of the entry point.

6 Gateways

While NG9-1-1 is defined to utilize an end-to-end IP architecture, there will continue to be wireline and wireless (circuit-switched) originating networks and legacy PSAPs deployed after emergency service networks and a significant number of PSAPs have evolved to support the i3 Solution. Since any i3 PSAP will need to be able to receive emergency calls that originate on these legacy networks, and legacy PSAPs will need to process voice emergency call originations that traverse ESInets, it is clear that gateways will be a required part of the i3 Solution architecture. The Legacy Network Gateway (LNG) is an i3 functional element that supports the interconnection of legacy originating networks and the ESInet. The Legacy PSAP Gateway (LPG) is a functional element that supports the interconnection of the ESInet with legacy PSAPs. Each of these gateways is comprised of a set of functional components. The placement of the gateways in the i3 Solution architecture, and the functional components that make up the Legacy Network Gateway and the Legacy PSAP Gateway, are illustrated in Figure 6-1. The following subsections

[56] The trusted root is the PCA for all entities within an ESInet, but in some cases (such as when a Logging Service is asked to log events that originated outside an ESInet) there may be a different trusted root.

© Copyright 2011-2022 National Emergency Number Association, Inc.

provide a detailed description of the functional components and interfaces that MUST be supported by a Legacy Network Gateway and a Legacy PSAP Gateway.

Note: Another component, a Legacy Selective Router Gateway (LSRG), is used as part of transition to i3. The LSRG is described in a separate document [114].

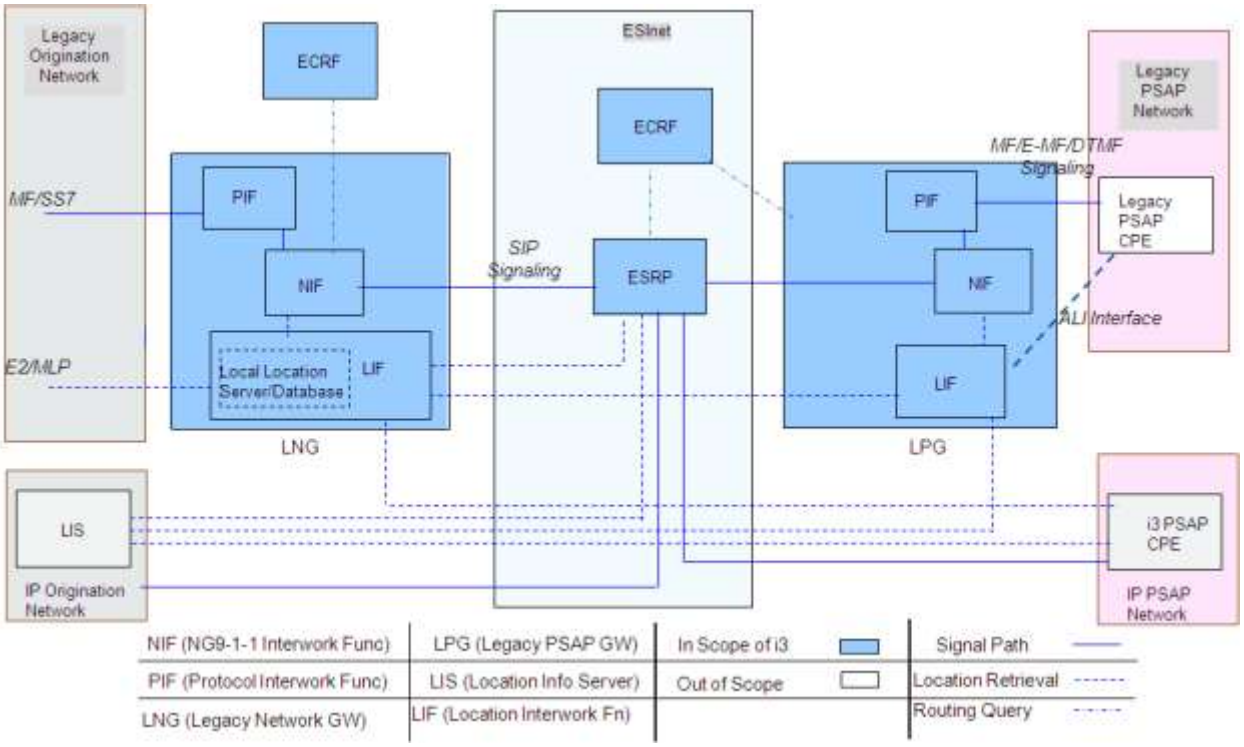


Figure 6-1 i3 Gateways – Functional Architecture

6.1 Legacy Network Gateway (LNG)

A Legacy Network Gateway is a signaling and media interconnection point between callers in legacy wireline/wireless originating networks and the i3 architecture. The Legacy Network Gateway logically resides between the originating network and the ESInet and allows i3 PSAPs to receive emergency calls from legacy originating networks. Calls originating in legacy wireline or wireless networks must undergo signaling interworking to convert the incoming Multi-Frequency (MF) or Signaling System Number 7 (SS7) signaling to the IP-based signaling supported by the ESInet. Thus, the Legacy Network Gateway supports a physical SS7 or MF interface on the side of the originating network, and an IP interface which produces SIP signaling towards the ESInet and MUST provide the protocol interworking functionality from the SS7 or MF signaling that it receives from the legacy originating network to the SIP signaling used in the ESInet.

© Copyright 2011-2022 National Emergency Number Association, Inc.

The Legacy Network Gateway is also responsible for routing emergency calls to the appropriate ESRP in the ESInet. To support this routing, the Legacy Network Gateway MUST apply specific interwork functionality to legacy emergency calls that will allow the information provided in the call setup signaling by the wireline switch or Mobile Switching Center (MSC) (e.g., calling number/ANI, ESRK, cell site/sector represented by an ESRD) to be used as input to the retrieval of location information from an associated location server/database. The Legacy Network Gateway uses this location information to query an ECRF to obtain routing information in the form of a URI. The Legacy Network Gateway MUST then forward the call/session request to an ESRP in the ESInet, using the URI provided by the ECRF**,** and include callback and location information in the outgoing signaling.

The Legacy Network Gateway functional element contains three functional components, as illustrated in Figure 6-1.[57] These functional components are described below:

1. (MF/SS7 to SIP) Protocol Interwork Function (PIF): This functional component performs a standard interworking function that converts the incoming MF signaling or SS7 protocol from the legacy network to the SIP protocol expected by the i3 ESInet and also converts the incoming TDM voice to the RTP data required by the i3 ESInet. If the incoming call is a TTY call, the PIF will be responsible for interworking TTY to real-time text per RFC 5194 [84]. It is assumed that the PIF functional component does not require specialized hardware and can therefore be implemented using commercially available hardware. (See Section 6.1.1 for further details.)
2. NG9-1-1-specific Interwork Function (NIF): This functional component provides NG9-1-1-specific processing of the incoming call signaling, which includes identification of the key(s) (e.g., calling number/ANI, ESRK, ESRD) that will be used as input to location retrieval. (See below for further information regarding the Location Interwork Function [LIF] functional component of the Legacy Network Gateway.) Having received the location information from the LIF, the NIF functional component provides the means by which the address of the target ESRP is identified (i.e., via a query to the ECRF), and the route to that ESRP is selected. This functional component also includes the ability to select a default route if necessary. Having identified the route to the ESRP, the NIF is also responsible for forwarding

[57] Note that the functional decomposition of the Legacy Network Gateway described in this section is provided to assist the reader in understanding the functions and external interfaces that a Legacy Network Gateway must support. Actual implementations may distribute the functionality required of the Legacy Network Gateway differently among functional components, as long as all of the functions and external interfaces described herein are supported.

© Copyright 2011-2022 National Emergency Number Association, Inc.

the request to the ESRP and including location and callback information in the outgoing SIP signaling. The NIF is also responsible for taking any non-location call information provided by the LIF and generating a data structure that contains Additional Data about the call, along with a pointer/reference to that data structure. (See Section 6.1.2 for further details.)

3. Location Interwork Function (LIF): This functional component is responsible for taking the appropriate key(s) from the incoming signaling (e.g., calling number/ANI, ESRK, ESRD), provided to it by the NIF, and using it (them) to retrieve location information via an associated location server/database[58]. The location information is provided to the NIF for use in determining the route for the emergency call, and for populating the outgoing SIP INVITE message. Other non-location information associated with the call that is known or obtained by the LIF will be passed to the NIF for population in an AdditionalData data structure. (See Section 6.1.3 for further details.)

When the LNG is provided by the 9-1-1 authority, or the NGCS operator, the LNG must implement the server-side of the ElementState event notification package.

The following subsections describe each of the functional components of the Legacy Network Gateway in detail.

Note: The LNG must log all significant events. Log record formats for this purpose are provided in Section 4.12.3 of this document.

6.1.1 Protocol Interwork Function (PIF)

To receive emergency calls from legacy originating networks, the Legacy Network Gateway is expected to support MF and SS7 trunking arrangements. Flexibility is required to accommodate different implementations for each type of interface.

6.1.1.1 MF Trunk Interface

If legacy wireline or wireless emergency calls are routed via MF trunks from the wireline end office or wireless MSC to the Legacy Network Gateway, the PIF component of the Legacy Network Gateway SHALL be capable of receiving and processing the following MF signaling:

[58] Note that, in the case of certain legacy wireless emergency call originations, the location server/database will need to query an element in the legacy wireless network (i.e., an MPC/GMLC) to obtain caller location associated with the emergency call.

© Copyright 2011-2022 National Emergency Number Association, Inc.

- The PIF component of the Legacy Network Gateway SHALL be capable of recognizing a trunk seizure and returning a wink back to the wireline switch or MSC.
- Upon receiving an MF digit string containing the dialed digits "911" (i.e., KP + 911 + ST), the PIF component SHALL return an ANI request signal to the wireline trunk or MSC.
- The PIF component of the Legacy Network Gateway SHALL be capable of receiving and processing the appropriate ANI sequence. If CAMA-type signaling is used on the MF trunk from a wireline end office to the Legacy Network Gateway, the PIF component of the Legacy Network Gateway SHALL be capable of receiving and processing an ANI sequence that consists of "I + 7-digit ANI".
- If Feature Group D operator-type signaling is used on the MF trunk from a wireline end office to the PIF component of the Legacy Network Gateway, the PIF component SHALL be capable of receiving and processing an ANI sequence consisting of "II + 7/10 digit ANI".
- If the Legacy Network Gateway receives an emergency call that originates in a wireless network and is routed over an MF trunk group from an MSC, the PIF component of the Legacy Network Gateway SHALL be capable of receiving and processing Feature Group D signaling as described below:
    - If an emergency call originates in a wireless network and is routed from an MSC to the Legacy Network Gateway over an MF trunk group, and an ESRD is outpulsed with the ANI, the PIF component of the Legacy Network Gateway SHALL be capable of receiving and processing "II+7/10 digit+10 digit" Feature Group D-type signaling, where ANI is outpulsed as the first 7/10 digit number, and ESRD is outpulsed as the second 10 digit number (i.e., the called party number).
    - If an emergency call originates in a Commercial Mobile Radio Service (CMRS)-type wireless network and is routed from an MSC to the Legacy Network Gateway over an MF trunk group, and the wireless network uses the Wireline Compatibility Mode approach (i.e., only the ESRK is signaled), the PIF component of the Legacy Network Gateway SHALL be capable of receiving and processing an ESRK following the "II" (i.e., as ANI), and the digits "9-1-1", "1-1", or "1" as the called number.
- Upon receiving a 200 OK message from the NIF component, the PIF component SHALL generate an answer signal to the wireline switch or MSC.
- The PIF component of the Legacy Network Gateway SHALL be capable of receiving and processing an on-hook indication from a wireline switch or MSC and shall generate a SIP BYE message toward the NIF, as described in Section 6.1.1.5.

© Copyright 2011-2022 National Emergency Number Association, Inc.

6.1.1.2 SS7 Interface

When a wireline end office or MSC determines that an SS7 Initial Address Message (IAM) associated with a 9-1-1 call is to be generated, it will also need to generate and pass some Message Transfer Part (MTP)-level information, along with the Integrated Services Digital Network User Part (ISUP) information, to the Legacy Network Gateway.

6.1.1.2.1 SS7 Message Transfer Part (MTP) Signaling for 9-1-1 Call Setup

The wireline end office/MSC will be responsible for generating information that will be populated in the MTP Signaling Information Field (SIF) and the Service Information Octet (SIO) portions of the IAM sent to the Legacy Network Gateway.

The SIO contains the service indicator that identifies the MTP user involved in the message. In the case of a call setup message generated by a wireline end office or MSC, the service indicator will identify the ISDN User Part as the MTP user. The subservice field will indicate that the message is a national network message and will identify the MTP message priority. In the case of IAMs related to 9-1-1 calls, the message priority will have the value "1" (where priority 3 is the highest priority assigned to SS7 messages)[59]. Therefore, the PIF component of the Legacy Network Gateway SHALL be capable of receiving and processing an IAM that contains MTP information that includes a Service Information Octet (SIO) that contains the following information:

- The service indicator SHALL identify the ISDN User Part as the MTP user.
- The subservice field SHALL indicate that the message is a national network message and that the message priority has a value of "1".

The SIF contains a routing label, consisting of the Originating and Destination Point Codes, as well as the Signaling Link Selection value for the message, a Circuit Identification Code associated with the trunk selected for the call, a Message Type Code identifying the message as an Initial Address Message (IAM), and the content of the IAM itself. The PIF component of the Legacy Network Gateway SHALL be capable of receiving and processing an IAM that contains MTP information that includes a Signaling Information Field (SIF) containing the following information:

- A routing label that contains the point code of the wireline end office or MSC in the Originating Point Code field, the point code of the Legacy Network Gateway in the Destination Point Code field, and an SLS code assigned by the wireline end office/MSC.

[59] Note that the MTP message priority does not determine which messages are processed first when received at a node but is used instead to determine which messages should be discarded if the SS7 network experiences congestion.

© Copyright 2011-2022 National Emergency Number Association, Inc.

- A Circuit Identification Code assigned by the wireline end office/MSC and associated with the trunk selected for the call.
- A Message Type code identifying the message as an IAM.
- The content of the IAM itself.

Further details related to MTP message structure can be found in GR-246-CORE [143], *Telcordia Technologies Specification of Signaling System Number 7,* Chapter T1.110.1, Section 5.1 and Chapter T1.111.3, Section 2.

6.1.1.2.2 SS7 ISUP Signaling for 9-1-1 Call Setup

This subsection describes requirements on the Legacy Network Gateway for processing ISUP signaling related to the receipt of emergency calls originated by legacy wireline and wireless customers over an SS7-controlled trunk. It is assumed that the trunk group from the wireline end office or MSC to the Legacy Network Gateway is a dedicated trunk group per carrier.

If the incoming trunk to the Legacy Network Gateway is an SS7-controlled dedicated trunk selected by a wireline end office or wireless MSC, the PIF component of the Legacy Network Gateway SHALL be capable of receiving and processing an ISUP IAM containing parameters populated as described in GR-2956-CORE [159], *CCS/SS7 Generic Requirements in Support of E9-1-1 Service,* Sections 5.2.1.2.1, R2956-77 and 5.2.1.4.1, R2956-82, respectively.

The PIF component of the Legacy Network Gateway SHALL also be capable of receiving and processing an ISUP Release (REL) message from a wireline end office or MSC, formatted as described in Table A-5 of GR-317-CORE [160], and generating a Release Complete Message (RLC) formatted as described in Table A-6 of GR-317-CORE in response. The PIF component of the Legacy Network Gateway SHALL also generate a SIP BYE message toward the NIF, as described in Section 6.1.1.5.

The PIF component of the Legacy Network Gateway SHALL be capable of receiving and processing supervisory ISUP messages sent by wireline end offices and MSCs (e.g., Blocking, Blocking Acknowledgement). The PIF component SHALL follow the procedures described in Section 3.1.4 of GR-317-CORE for processing these messages.

6.1.1.3 Early Media

In order to provide the equivalent of "trunk-side recording", an LNG is expected to provide Early Media to downstream elements whenever it is possible to do so (for example, with an MF trunk origination). Any LNG that is acting as a SIPREC (RFC 5766) [119] SRC (Session Recording Client) SHALL provide Early Media (RFC 3960) [30] to the SRS (Session Recording Server).

© Copyright 2011-2022 National Emergency Number Association, Inc.

6.1.1.4 Handling of Media Associated with TTY Calls

If the Legacy Network Gateway receives an incoming TTY call, the PIF component will be responsible for recognizing the Baudot tones in incoming media and replacing them with RFC 4103 [85] real-time text. Likewise, the PIF component will be responsible for generating Baudot tones in outgoing media (i.e., toward the caller) if real-time text is received in RTP packets, as described below.

The Legacy Network Gateway SHALL handle a TTY emergency origination by establishing an audio session with the PSAP and subsequently requesting, or processing an incoming request for, the addition of an RFC 4103 text media session as described below.

If the emergency call is delivered to the PSAP as a "silent" call, the Legacy Network Gateway MUST be capable of receiving and processing a re-INVITE from an i3 PSAP or Legacy PSAP Gateway that requests the addition of RFC 4103 text media to the existing emergency session.

If the PIF component detects Baudot tones from the caller after an audio session is established, and an RFC 4103 text media session has not already been established (via a re-INVITE from an i3 PSAP or Legacy PSAP Gateway), the PIF component SHALL generate a SIP re-INVITE message that includes an offer in the SDP describing a media format associated with real-time text (as specified in RFC 4103) and send the SIP re-INVITE message to the NIF component. The PIF component will buffer any real-time text that is converted from the received Baudot tones until such time as the real-time text media session is established (i.e., a 200 OK message is received from the NIF component in response to the re-INVITE) and the real-time text can be passed forward. (See Section 6.1.1.5 for further details.)

If the PIF component detects Baudot tones from the caller before an audio session is established, the PIF component SHALL wait for the audio session to be established, and if a text session has not already been established, the PIF SHALL generate a SIP re-INVITE message that includes an offer in the SDP describing a media format associated with real-time text (as specified in RFC 4103) and send the SIP re-INVITE message to the NIF component. The PIF component will buffer any real-time text that is converted from the received Baudot tones until such time as the real-time text media session is established (i.e., a 200 OK message is received from the NIF component in response to the re-INVITE) and the real-time text can be passed forward. (See Section 6.1.1.5 for further details.)

If the PIF component receives (i.e., from a legacy PSAP/LPG) simultaneous RFC 4103 real-time text and audio media that may include Baudot tones or other sounds, the PIF component MUST notch the audio frequencies used for Baudot tones from the received audio media and then insert the Baudot tones transcoded from the received RFC 4103 text to minimize the distortion of the Baudot tones delivered to the caller. When transcoding

© Copyright 2011-2022 National Emergency Number Association, Inc.

from RFC 4103 text to Baudot tones, the LNG SHALL support the special character mappings described in Section 6.2.1.4

6.1.1.5 Internal Interface to the NIF Component

The PIF component of the Legacy Network Gateway MUST have the capability to use standard interworking procedures**,** as defined in ATIS-1000679.2015 [130]**,** to generate a SIP INVITE message based on incoming SS7 signaling and pass that INVITE message to the NIF component of the Legacy Network Gateway. The PIF component MUST also support mappings from MF signaling sequences to the appropriate fields in the outgoing SIP INVITE message, as described below.

The initial SIP INVITE message generated by the PIF SHALL consist of the following information:

- A Request-URI that contains the information signaled in the SS7 Called Party Number parameter (per ATIS-1000679.2015) or as the MF called number.
- A To header field that contains the information signaled in the SS7 Called Party Number parameter (per ATIS-1000679.2015) or as the MF called number.
- A From header field that contains the information signaled in an SS7 Generic Digits Parameter (GDP), if present.

  If a GDP is not received in incoming signaling, the From header field will be populated with the information signaled in the SS7 Calling Party Number parameter (if present).
- A P-Asserted-Identity (P-A-I) header field that is populated with the information contained in the SS7 Calling Party Number parameter (per ATIS-1000679.2015). In addition, the P-A-I header field will also contain the content of the SS7 Calling Party Category (CPC) parameter and the Originating Line Information (OLI) parameter, if present in the received SS7 Initial Address Message (IAM) (per ATIS-1000679.2015).
- A P-Charge-Info header field that is populated with the information that was contained in the SS7 Charge Number parameter (per ATIS-1000679.2015) or was signaled as the MF ANI.
- A Contact header field that contains the trunk group parameters that identify the ingress trunk group to the Legacy Network Gateway, as defined in RFC 4904 [161].
- A Via header field that is populated with the Element Identifier (see Section 2.1.3) for the Legacy Network Gateway.
- An SDP offer that includes the G.711 codec.

The PIF component of the Legacy Network Gateway SHALL be capable of receiving and processing a SIP Trying (100) message passed to it by the NIF component, acknowledging receipt of the INVITE that was previously generated by the PIF component.

© Copyright 2011-2022 National Emergency Number Association, Inc.

The PIF component of the Legacy Network Gateway SHALL also be capable of receiving and processing a 180 Ringing message that contains either a "text" media feature tag or a "urn:emergency:media-feature.tty-interworking" media feature tag. (A 183 Session Progress message with a "urn:emergency:media-feature.tty-interworking" media feature tag will be received by the PIF component if the destination PSAP is an i3 PSAP.) If the incoming trunk group to the Legacy Network Gateway is an SS7 trunk group, then upon receiving the 180 Ringing message, the PIF component of the Legacy Network Gateway SHALL generate an ISUP Address Complete Message (ACM) formatted as described in Section 7.2.1.1 of ATIS-1000679.2015 [130] and Section 3.1.1.5 of GR-317-CORE, *LSSGR: Switching System Generic Requirements for Call Control Using the Integrated Services Digital Network User Part (ISDNUP),* with the following clarification: It is expected that bits DC of the Backward Call Indicator parameter SHOULD be set to "01" indicating "subscriber free", bits HG of the Backward Call Indicator parameter SHOULD be set to "00" indicating "no end-to-end method available", bit I SHALL be set to "1" indicating "interworking encountered"," bit K SHALL be set to "0" indicating "ISDN User Part not used all the way", and bit M SHALL be set to "0" indicating "terminating access non-ISDN".

The PIF component of the Legacy Network Gateway SHALL be capable of receiving and processing a 183 Session Progress message that contains a "text" media feature tag. (This message will be received by the PIF component if the destination PSAP is a legacy PSAP.) If the incoming trunk group to the Legacy Network Gateway is an SS7 trunk group, then upon receiving the 183 Session Progress message, the PIF component of the Legacy Network Gateway SHALL generate an ISUP Address Complete Message (ACM) formatted as described in Section 7.2.1.1 of ATIS-1000679.2015 [130] and Section 3.1.1.5 of GR-317-CORE, LSSGR: Switching System Generic Requirements for Call Control Using the Integrated Services Digital Network User Part (ISDNUP), with the following clarification: It is expected that bits DC of the Backward Call Indicator parameter SHOULD be set to "00" indicating "no indication", bits HG of the Backward Call Indicator parameter SHOULD be set to "00" indicating "no end-to-end method available", bit I SHALL be set to "1" indicating "interworking encountered", bit K SHALL be set to "0" indicating "ISDN User Part not used all the way", and bit M SHALL be set to "0" indicating "terminating access non-ISDN". The Optional Backward Call Indicators parameter SHALL also be included in the ACM, with the "inband information indicator" (Bit A) set to "1" indicating "inband information or an appropriate pattern is now available".

The PIF component of the Legacy Network Gateway SHALL be capable of receiving and processing a 200 OK message, indicating that the call has been answered. If the incoming trunk to the Legacy Network Gateway is an SS7 trunk, then upon receiving the 200 OK message, the PIF SHALL generate an ISUP Answer Message (ANM) formatted as described in Section 3.1.1.6 of GR-17-CORE. If ANM is the first backward message sent by the Legacy Network Gateway (i.e., no ACM is sent previously due to the 200 OK being the first

© Copyright 2011-2022 National Emergency Number Association, Inc.

SIP message received), the Legacy Network Gateway SHALL follow the procedures specified in Section 7.5.1 of ATIS-1000679.2015. Specifically, the Called Party's Status indicator (Bit DC) of the Backward Call Indicators parameter SHALL be set to "no indication," bit I SHALL be set to "1" indicating "interworking encountered," bit K SHALL be set to "0" indicating "ISDN User Part not used all the way," and bit M SHALL be set to "0" indicating "terminating access non-ISDN."

If the incoming trunk to the Legacy Network Gateway is an MF trunk, then upon receiving the 200 OK message, the PIF SHALL generate an answer signal to the wireline switch or MSC.

As described in Section 6.1.1.4, if the PIF component subsequently detects Baudot tones associated with a TTY origination, and a real-time text media session has not already been established for the emergency call (due to receipt of a re-INVITE generated by an i3 PSAP or Legacy PSAP Gateway or egress LSRG), the PIF component SHALL generate a SIP re-INVITE message that includes an SDP offer associated with real-time text, and send it to the NIF component. The re-INVITE message SHALL reference the existing dialog so that the i3 PSAP (or Legacy PSAP Gateway, or egress LSRG, in the case of a legacy PSAP) knows that it is requesting modification of an existing session instead of establishing a new session. The re-INVITE message SHALL include the same information as the original SIP INVITE message generated by the PIF component, with the exception that the SDP offer will include a media format associated with real-time text, as described in RFC 4103 [85].

The PIF component SHALL wait to receive a 200 OK message from the NIF component indicating that the offer of real-time text has been accepted before sending the text media forward. The PIF component SHALL respond to the 200 OK by returning an ACK message.

The PIF component MUST be capable of receiving and processing re-INVITE messages from the NIF component associated with emergency calls that are presented to the PSAP as a "silent" call. The received re-INVITE message will include an offer of a media format associated with real-time text (as described in RFC 4103 [85]). This re-INVITE message will include the following information:

- A Request-URI that contains the URI and trunk group parameters delivered to the NIF component in the Contact header field of the initial INVITE message.
- A To header field that contains the information signaled in the From header field of the original INVITE message (i.e., the information signaled in an SS7 GDP, if present, or the information signaled in the SS7 Calling Party Number parameter).
- A From header field that contains the digits "911" expressed as a URI (delivered to the NIF component in the To header field of the original INVITE message).
- A Contact header field that contains the information signaled to the NIF in the Request-URI of the original INVITE message (i.e., the digits contained in the SS7

© Copyright 2011-2022 National Emergency Number Association, Inc.

Called Party Number parameter (e.g., "911" expressed as a URI) and either a 'text' media feature tag or a "urn:emergency:media-feature.tty-interworking" media feature tag.

- A Via header field that is populated with a URI associated with the i3 PSAP or Legacy PSAP Gateway or egress LSRG.
- An SDP offer that includes a media format associated with real-time text, as described in RFC 4103 [85].

Upon receiving the re-INVITE message from the NIF component, the PIF SHALL respond with a 200 OK message, indicating that it accepts the SDP offer associated with real-time text. It SHALL be capable of receiving an ACK from the NIF component in response.

The PIF component of the Legacy Network Gateway SHALL be capable of receiving and processing a SIP BYE message and acknowledging the BYE by returning a 200 OK message to the NIF. If the incoming trunk to the Legacy Network Gateway is an SS7 trunk, then upon receipt of the BYE message, the PIF SHALL generate an ISUP REL message, and be capable of receiving and processing an ISUP RLC sent in response. If the incoming trunk to the Legacy Network Gateway is an MF trunk, then upon receipt of the BYE message, the PIF SHALL generate an on-hook signal to the wireline switch or MSC.

The PIF SHALL also be capable of generating a BYE message and sending it to the NIF if an ISUP REL is received from the wireline switch or MSC or an on-hook signal is received over an MF trunk from the wireline switch or MSC and SHALL be capable of receiving and processing a 200 OK message from the NIF sent in acknowledgement.

In support of emergency call transfer procedures, the PIF component of a Legacy Network Gateway SHALL be capable of receiving and processing an INVITE method containing a conference URI, isfocus, and a Replaces header field that references the leg between the Legacy Network Gateway and the Primary (transfer-from) PSAP, from the NIF component. (See Section 6.1.2.2 for further discussion.) The PIF component SHALL respond to this SIP INVITE by returning a 200 OK, and SHALL receive an ACK from the NIF component in response to the 200 OK. The PIF component SHALL generate a BYE message to terminate the session with the Primary PSAP and send it to the NIF component. At this point, the Legacy Network Gateway switches the media from the session with the transfer-from PSAP to the session with the bridge.

The PIF component of the Legacy Network Gateway SHALL be capable of receiving and processing a 200 OK message from NIF component in response to the BYE message. At this point the session between the Legacy Network Gateway and the transfer-from PSAP is terminated.

If the ESInet supports the transfer models described in Sections 4.7.1.1 or 4.7.1.2, the PIF component of the Legacy Network Gateway SHALL be capable of receiving and processing

© Copyright 2011-2022 National Emergency Number Association, Inc.

a SIP INVITE from the NIF component that contains a Replaces header that requests that the connection to the bridge be replaced with a connection to the transfer-to PSAP. The PIF component SHALL respond to this SIP INVITE by returning a 200 OK and SHALL receive an ACK from the NIF component in response to the 200 OK. The PIF component SHALL generate a BYE message to terminate the session with the bridge and send it to the NIF component. At this point, the Legacy Network Gateway switches the media from the session with the bridge to the session with the transfer-to PSAP. The PIF component of the Legacy Network Gateway SHALL be capable of receiving and processing a 200 OK message from NIF component in response to the BYE message. At this point the session between the Legacy Network Gateway and the conference bridge is terminated.

Note that if the PIF does not support INVITE/Replaces, the NIF MAY complete processing of INVITE/Replaces instead of the PIF.

If the PIF component receives other SIP messages from the NIF component, it SHALL process them per RFC 3261 [10].

6.1.2 NG9-1-1-specific Interwork Function (NIF)

6.1.2.1 NIF Handling of INVITE from PIF

The NIF component of the Legacy Network Gateway functional element is expected to provide special processing of the information received in the incoming INVITE message from the PIF component to facilitate call delivery to an i3 ESInet. The NIF SHALL determine, based on the incoming trunk group and/or the incoming signaling, whether the call is a wireline or wireless emergency call. If the call is received over an MF trunk group, the NIF SHALL make this determination based on the incoming trunk group parameters included in the Contact header field of the INVITE message from the PIF. If the call is received over an SS7 trunk group, the NIF SHALL make this determination based on the coding of the cpc and oli parameters in the P-A-I header field of the INVITE message from the PIF and/or the ingress trunk group parameters in the Contact header field of the INVITE message from the PIF. Based on this determination, the NIF SHALL extract the appropriate information (i.e., calling party number, charge number, and/or ESRD) from the incoming signaling to be used as the location key and SHALL pass it to the Location Interwork Function (LIF) for use in obtaining caller location information. (See Section 6.1.3 for further discussion of LIF functionality and interfaces.)

If the NIF determines that the incoming call is a legacy wireline emergency call, and only one number is received in incoming signaling as the Calling Party Number (CPN)/ANI (i.e., the URI in the From, P-A-I, and P-Charge-Info header fields of the INVITE message received from the PIF contains the same CPN/ANI), the NIF SHALL pass this number to the

© Copyright 2011-2022 National Emergency Number Association, Inc.

LIF to use in retrieving the location for the call[60]. If the NIF determines that the incoming call is a legacy wireline emergency call and two different numbers are received in incoming signaling (i.e., the INVITE message from the PIF contains a URI associated with the Charge Number in the P-Charge-Info header field and a different URI associated with the CPN in the P-A-I header field) the NIF MUST support a configuration option to tell it which number to send to the LIF as input to location retrieval.

If the NIF determines (based on the oli parameter in the P-A-I header field or the trunk group information in the Contact header field) that the incoming call is a legacy wireless emergency call, and both a callback number (i.e., Mobile Directory Number [MDN]) and an ESRD are received in incoming signaling, the NIF SHALL send both numbers to the LIF since both are required to uniquely identify the call. The NIF will determine, based on configured information associated with the trunk group identified in the trunk group parameters within the Contact header field of the received INVITE, where to extract the callback information and ESRD from. The ESRD MAY be populated in the Request-URI/To header fields or in the From header field. The MDN MAY be populated in the From header field or the P-A-I header field.

(See Section 6.1.3 for further discussion of what the LIF does with this information.)

6.1.2.1.1 NIF Handling of Location Information from the LIF

Once the NIF receives location information from the LIF in geodetic or civic format, the NIF MUST be capable of generating a routing request to an ECRF. The NIF SHALL generate a LoST query, which includes the location information provided by the LIF and an appropriate service URN (i.e., "urn:service:sos"), following the procedures described in Section 3.4. If the NIF does not receive a routing location from the LIF component within a pre-specified period of time, the NIF component SHALL use a default location (based on the incoming trunk group information provided in the Contact header field of the INVITE message from the PIF component) to query the ECRF.

Upon receiving the response from the ECRF, the NIF SHALL determine the outgoing route for the call using the URI of the target ESRP received in the LoST response. If the NIF component of the Legacy Network Gateway does not receive a response to a LoST query within a provisioned time period, or receives an error indication from the ECRF, it SHALL log the event and route the call based on a provisioned default ESRP URI.

---

[60] Note that this processing will also apply to wireless Wireline Compatibility Mode calls, since these are marked as wireline in incoming signaling and contain a single 10-digit number, the ESRK, which is signaled as the SS7 CPN or MF ANI.

© Copyright 2011-2022 National Emergency Number Association, Inc.

In addition to determining the outgoing route, the NIF may generate a data structure that contains Additional Data about the call. The data structure SHALL contain the mandatory information identified in Section 3.1 of NENA 71-001 [73], as well as any other non-location information associated with the call that is provided to the NIF by the LIF, formatted according to RFC 7852 [107]. The NIF may include this Additional Data (or a subset of it) "by-value" in the body of the outgoing SIP message it sends to the ESRP, and/or it may generate a pointer/reference to that data structure. The pointer SHALL contain the URI of the ADR in which the Additional Data information is stored. The URI generated by the NIF SHOULD include the callback number. If there is only static information and no per-call information, the NIF MAY include a reference URI to a static ADR that may be maintained at the NIF or elsewhere if maintained by the 9-1-1 Authority. If the NIF generates a pointer/reference to an Additional Data structure (or passes Additional Data by value), it SHALL include the reference URI (which may be a CID) in the Call-Info header field of the INVITE message sent to the ESRP, with a purpose parameter beginning with "EmergencyCallData", a dot and the block name of the Additional Data structure. If the NIF passes Additional Data by reference, and the reference refers to the LNG, the NIF component of the LNG MUST maintain an ADR interface, utilizing the HTTPS GET method described in IETF RFC 7230 [162], to support dereference requests for Additional Data.

6.1.2.2 SIP Interface to the ESInet

The NIF is expected to behave as a B2BUA and generate a SIP INVITE message to be sent to the ESRP. This initial INVITE message SHALL contain information received in the initial INVITE message from the PIF component, as well as location and possibly callback information received from the LIF component. The initial INVITE message MAY also contain reference URIs associated with any Additional Data structures generated by the NIF, if any are generated.

If a default location was used to query the ECRF, the SIP INVITE message generated by the NIF component SHALL include a PIDF-LO document in the body that contains the default location with a <method> element set to the value "Default", and the <provided-by> element set to the identity of Legacy Network Gateway provider that inserted it, and a Geolocation header field populated with a "cid" URI pointing to it.

The INVITE message generated by the NIF component of the Legacy Network Gateway SHALL contain the following information:

- A Request-URI that contains a service URN in the "sos" tree (i.e., "urn:service:sos")
- A To header field that contains the digits "911"
- A From header field that contains the callback number (or Originating TN for legacy wireline emergency call originations) received by the NIF component in incoming

© Copyright 2011-2022 National Emergency Number Association, Inc.

signaling from the PIF component, or retrieved by the LIF component, as appropriate for the type of emergency call origination.

- If the "Service Delivered by Provider to End User" provided by the LIF component is equal to "POTS," the NIF component SHALL populate the From header field based on the Calling Party Number received in the From and P-A-I header fields of the incoming INVITE message from the PIF component.
- If the "Service Delivered by Provider to End User" provided by the LIF component is equal to "wireless", then the NIF component SHALL populate the From header field as follows:
  - If the From header field and the P-A-I header field of the incoming INVITE message from the PIF component are not the same (i.e., a GDP was received in the incoming signaling from the MSC), the NIF component SHALL use the value provided in the P-A-I header field of the INVITE message from the PIF component to populate the From header field of the outgoing INVITE message.
  - If the From header field and the P-A-I header field of the incoming INVITE message from the PIF component are the same (i.e., no GDP was present in the incoming signaling from the MSC), the NIF component SHALL use the callback number provided by the LIF component to populate the From header field of the outgoing INVITE message. If the LIF component does not provide a callback number to the NIF component within a pre-specified period of time, the NIF component SHALL populate the From header field with the value received in the incoming INVITE message from the PIF component.
- If the call was originated by a non-initialized mobile caller (i.e., the callback number is of the form 911**+** "last 7 digits of the ESN or IMEI expressed as a decimal") the From header field SHALL contain a value of "Anonymous."

- A P-Asserted-Identity (P-A-I) header field that contains the callback number retrieved by the LIF component or received in incoming signaling from the PIF component, as appropriate for the type of emergency call origination. Note that the P-A-I sent by the NIF component to the ESRP will not contain cpc or oli parameters.
  - If the "Service Delivered by Provider to End User" provided by the LIF component is equal to "POTS," the NIF component SHALL populate the P-A-I with the SS7 Calling Party Number information received in the P-A-I header field of the incoming INVITE message from the PIF component.
  - If the "Service Delivered by Provider to End User" provided by the LIF component is equal to "wireless", then the NIF component SHALL populate the P-A-I header field as follows:

© Copyright 2011-2022 National Emergency Number Association, Inc.

        - If the From header field and the P-A-I header field of the incoming INVITE message from the PIF component are not the same (i.e., a GDP was received in the incoming signaling from the MSC), the NIF component SHALL use the SS7 Calling Party Number value provided in the P-A-I header field of the INVITE message from the PIF component to populate the P-A-I header field of the outgoing INVITE message.
        - If the From header field and the P-A-I header field of the incoming INVITE message from the PIF component are the same (i.e., no GDP was present in the incoming signaling from the MSC), the NIF component SHALL use the callback number provided by the LIF component to populate the P-A-I header field of the outgoing INVITE message. If the LIF component does not provide a callback number to the NIF component within a pre-specified period of time, the NIF component SHALL omit the P-A-I header field from the outgoing INVITE message.
    - If a non-initialized mobile caller originated the call, the P-A-I header field SHALL be omitted.
- A P-Charge-Info header field, if one was received in the INVITE message from the PIF component. This field will contain the information received by the Legacy Network Gateway in an SS7 Charge Number parameter or signaled as an MF ANI.
- A Via header field that is populated with the Element Identifier (see Section 2.1.3) for the Legacy Network Gateway
- A Route header field that contains the ESRP URI obtained from the ECRF (this URI should be augmented with the "lr" parameter in the Route header field to avoid Request-URI rewriting)
- A Contact header field that contains a SIP URI that is associated with the Legacy Network Gateway, along with a "urn:emergency:media-feature.tty-interworking" media feature tag.
- A Supported header field that contains the "geolocation-sip" option tag
- A Geolocation header field that either:
    - Points to the message body (using a "Content Identifier" URI, as defined in RFC 2392 [132]) where a PIDF-LO containing the location value retrieved by the LIF is coded (see Section 6.1.3 and RFC 6442 [8])[61] , or;
    - Contains a location-by-reference URI[62].

[61] This method SHALL be used for wireline emergency calls or default-routed calls.

[62] This method SHALL be used for wireless Phase 1 and Phase 2 calls to allow the queries for routing location as well as for initial and updated caller location.

© Copyright 2011-2022 National Emergency Number Association, Inc.

- A Geolocation-Routing header field set to "yes"
- An SDP offer as received from the PIF component.
- If, during the processing of the emergency call, the NIF component of the Legacy Network Gateway creates an Additional Data data structure and stores it, the NIF component of the Legacy Network Gateway SHALL include one or more[63] Call-Info header fields with a purpose parameter beginning with "EmergencyCallData", a dot and the block name of the Additional Data structure; a value set to the URI associated with the ADR that contains the Additional Data data structure which, when dereferenced, yields the Additional Data data structure.
- If, during the processing of the emergency call, the NIF component of the Legacy Network Gateway creates one or more AdditionalData structures and sends them forward by value in the outgoing INVITE message, the NIF component of the Legacy Network Gateway:
    - SHALL populate each data structure as a body part of the INVITE message with a MIME type of "Application/EmergencyCallData", a dot and the block name of Additonal Data.
    - For each Additional Data structure, SHALL include a Call-Info header field with a purpose parameter set to "EmergencyCallData.", a dot and the block name of the Additional Data, and a value set to the cid: URI that points to the body part containing the Additional Data.
    - Each Additional Data structure is contained in one body part and referenced by one Call-Info header field that identifies the block type and the CID.
- A P-Preferred-Identity header field populated with 911 + "last 7 digits of the ESN or IMEI expressed as a decimal" if the call was originated by a non-initialized mobile caller.

After sending the SIP INVITE to the ESInet, the NIF SHALL return a SIP Trying (100) message to the PIF.

The NIF component SHALL be capable of receiving and processing a 180 Ringing message or a 183 Session Progress message that includes a Contact header field with either a "text" media feature tag or a "urn:emergency:media-feature.tty-interworking" media feature tag from the ESInet in response to the SIP INVITE. If the NIF component receives a 180 Ringing message, it SHALL send a 180 Ringing message to the PIF component. If the NIF

[63] The NIF MUST add at least ProviderInfo and ServiceInfo and MAY add SubscriberInfo blocks as described in Section 4.11. These MAY be referenced in one Call-Info header field with multiple URIs or multiple Call-Info header fields with one or more URIs.

© Copyright 2011-2022 National Emergency Number Association, Inc.

component receives a 183 Session Progress message, it SHALL send a 183 Session Progress message to the PIF component.

The NIF component SHALL also be capable of receiving and processing a 200 OK message from the ESInet. If the NIF component receives a 200 OK message from the ESInet, it SHALL send it to the PIF component. The NIF component SHALL be capable of receiving and processing an ACK message from the PIF component in response to the 200 OK message. The NIF component SHALL subsequently send an ACK message to the ESInet.

If callback information is not available at the time that the initial INVITE message is sent by the NIF component to the ESRP, but is subsequently provided by the LIF component, the NIF component SHALL generate a re-INVITE message to communicate this information to the PSAP. The re-INVITE message SHALL reference the existing dialog so that the i3 PSAP (or Legacy PSAP Gateway or egress LSRG, in the case of a legacy PSAP) knows that it is to modify an existing session instead of establishing a new session. The re-INVITE message SHALL include the following information:

- A Request-URI that contains the information provided in the Contact header field of the 200 OK message that was returned in response to the original INVITE message;
- A To header field that contains the same information as the original INVITE message (i.e., the digits "911");
- A From header field that contains the same information as in the original INVITE message (i.e., the From header field will be populated with the value received in the incoming INVITE message from the PIF component, which is the ESRK);
- A P-Asserted-Identity (P-A-I) header field that contains the callback number retrieved by the LIF component;
- A Via header field that is populated with the Element Identifier (see Section 2.1.3) for the Legacy Network Gateway;
- A Route header field that contains the same information as in the original INVITE (i.e., the ESRP URI obtained from the ECRF, which should be augmented with the "lr" parameter to avoid Request-URI rewriting);
- A Contact header field that contains the same information as in the original INVITE message (i.e., a SIP URI associated with the Legacy Network Gateway along with a "urn:emergency:media-feature.tty-interworking" media feature tag).

Likewise, if the NIF component receives a re-INVITE message from the PIF component (because the PIF component has detected Baudot tones after the initial session was established), the NIF component SHALL send a re-INVITE message toward the PSAP requesting the establishment of a real-time text media session. The re-INVITE message SHALL include the following information:

- A Request-URI that contains the information provided in the Contact header field of the 200 OK message that was returned in response to the original INVITE message;

© Copyright 2011-2022 National Emergency Number Association, Inc.

- A To header field that contains the same information as the original INVITE message (i.e., the digits "911");
- A From header field that contains the same information as in the original INVITE message;
- A P-Asserted-Identity (P-A-I) header field that contains the callback number included in the previous INVITE message;
- A Via header field that is populated with the Element Identifier (see Section 2.1.3) for the Legacy Network Gateway;
- A Route header field that contains the same information as in the original INVITE (i.e., the ESRP URI obtained from the ECRF, which should be augmented with the "lr" parameter to avoid Request-URI rewriting);
- A Contact header field that contains the same information as in the original INVITE message (i.e., a SIP URI associated with the Legacy Network Gateway along with a along with a "urn:emergency:media-feature.tty-interworking" media feature tag);
- An SDP offer that includes a media format associated with real-time text, as described in RFC 4103 [85].

The i3 PSAP/Legacy PSAP Gateway/egress LSRG SHALL return a 200 OK to indicate that it accepts the change, and the Legacy Network Gateway SHALL respond to the 200 OK by returning an ACK message.

The NIF component MUST also be capable of receiving and processing a re-INVITE message sent by an i3 PSAP or Legacy PSAP Gateway or LSRG. This will occur if a "silent" call is received by the PSAP, and the PSAP attempts to establish communication using TTY/RTT (as specified in the SOP that specifies the handling of silent calls). The re-INVITE generated by the i3 PSAP/Legacy PSAP Gateway/LSRG SHALL request the addition of RFC 4103 text media to the emergency session already established with the Legacy Network Gateway. (See Section 6.2.2.4 for details related to the content of this re-INVITE message when generated by a Legacy PSAP Gateway/LSRG.) Upon receiving the re-INVITE from the i3 PSAP/Legacy PSAP Gateway, the NIF component SHALL send a re-INVITE message to the PIF component, as described in Section 6.1.1.5 The PIF component SHALL return a 200 OK indicating that it accepts the change, and the NIF component SHALL respond to the 200 OK by returning an ACK message. The NIF component SHALL also send a 200 OK message to the i3 PSAP/Legacy PSAP Gateway/LSRG, and the i3 PSAP/Legacy PSAP Gateway/LSRG SHALL return an ACK.

The NIF component SHALL be capable of receiving and processing a BYE message from the ESInet. If the NIF component receives a BYE message from the ESInet, it SHALL pass it to the PIF component. The NIF component SHALL be capable of receiving and processing a 200 OK message from the PIF component in response to the BYE message and SHALL subsequently send a 200 OK message to the ESInet.

© Copyright 2011-2022 National Emergency Number Association, Inc.

If the NIF component receives other SIP messages from the ESInet, it SHALL validate them and if necessary, apply the appropriate error handling per RFC 3261 [10]. If the messages pass the validity checks, the NIF component SHALL pass them to the PIF component.

The NIF component SHALL be capable of receiving and processing a BYE message from the PIF component. If the NIF component receives a BYE message from the PIF component, it SHALL send a BYE message to the ESInet. Upon receiving a 200 OK message from the ESInet in response to the BYE message, the NIF component SHALL return a 200 OK message to the PIF component.

In support of emergency call transfer procedures, the NIF component of a Legacy Network Gateway SHALL be capable of receiving and processing an INVITE method containing a conference URI, isfocus, and a Replaces header field that references the leg between the Legacy Network Gateway and the transfer-from PSAP, from a conference bridge in the ESInet. The NIF component SHALL pass the INVITE with Replaces to the PIF component. Upon receiving a 200 OK from the PIF component, the NIF component SHALL send an ACK to the PIF component and SHALL send a 200 OK to the conference bridge. The conference bridge will respond by returning an ACK to the NIF component.

At this point, a session is established between the Legacy Network Gateway and the conference bridge. Note that the media session between the Legacy Network Gateway and the transfer-from PSAP still exists at this time. Note also that the media between the caller and the Legacy Network Gateway is undisturbed.

The Legacy Network Gateway SHALL terminate the session with the transfer-from PSAP by sending a BYE message from the PIF component to the NIF component and on to the transfer-from i3 PSAP or LPG or LSRG, following the signaling path established by the INVITE request associated with the original emergency session. At this point, the Legacy Network Gateway switches the media from the session with the transfer-from PSAP to the session with the bridge.

The NIF component of the Legacy Network Gateway SHALL be capable of receiving and processing a 200 OK message from the transfer-from i3 PSAP/LPG/LSRG in response to the BYE message. Upon receiving a 200 OK from the transfer-from i3 PSAP/LPG/LSRG, the NIF component SHALL forward the 200 OK message to the PIF component. At this point the session between the Legacy Network Gateway and the transfer-from PSAP is terminated.

If the ESInet supports the transfer models described in Sections 4.7.1.1 or 4.7.1.2, the NIF component of the Legacy Network Gateway SHALL also be capable of receiving and processing a SIP INVITE from the transfer-to PSAP that contains a Replaces header that requests that the connection from the Legacy Network Gateway to the bridge be replaced with a connection to the transfer-to PSAP. The NIF component SHALL pass the INVITE with Replaces to the PIF component. Upon receiving a 200 OK from the PIF component, the NIF

© Copyright 2011-2022 National Emergency Number Association, Inc.

component SHALL send an ACK to the PIF component and SHALL send a 200 OK to the transfer-to PSAP. The transfer-to PSAP will respond by returning an ACK to the NIF component.

At this point, a session is established between the Legacy Network Gateway and the transfer-to PSAP. Note that the media session between the Legacy Network Gateway and the conference bridge still exists at this time. Note also that the media between the caller and the Legacy Network Gateway is undisturbed.

The Legacy Network Gateway SHALL terminate the session with the conference bridge by sending a BYE message from the PIF component to the conference bridge, following the signaling path established by the INVITE with Replaces previously received from the conference bridge. At this point, the Legacy Network Gateway switches the media from the session with the conference bridge to the session with the transfer-to PSAP.

Note that if the PIF does not support INVITE/Replaces, the NIF MAY complete processing of INVITE/Replaces instead of the PIF.

6.1.2.3 Handling of Media Associated with TTY Emergency Originations

As described in Section 6.1.1.4, the PIF component of the Legacy Network Gateway is responsible for interworking between Baudot tones and RFC 4103 text. To support this interworking, the NIF component MUST be capable of processing re-INVITE messages either received from the PIF component or from the PSAP or Legacy PSAP Gateway or egress LSRG via the ESInet (i.e., for "silent" calls) that contain an SDP offer for RFC 4103 real-time text. (See Section 6.1.1.5 for further discussion of the content of these re-INVITE messages.)

In addition, the NIF component SHALL be responsible for supporting the "turn-taking" conventions expected in TTY communications. When a TTY caller is sending characters, (i.e., it is the TTY caller's "turn"), the Baudot tones are converted to RFC 4103 characters and forwarded by the NIF to the ESInet. The NIF buffers any RFC 4103 characters it receives from the ESInet. When a "_GA"[64] (where the underscore indicates a space character) is received from the caller via the PIF, the NIF component will set an inter-character timer of 1500 ms. If a space or line delimiter is received, or the 1500 ms timer expires without any other character being received, the NIF will recognize that a change in turn is in effect. The NIF SHALL perform one of the following procedures, depending on the

[64] It is a convention with TTY to use the characters "GA" for "Go Ahead" at the end of the typed message when one user wants to give a turn to the other user. The following should also be interpreted as end of message values to address scenarios where there is a lost shift character: "+-" and "<BELL>)" (where the bell-character is U+0007 when converted to RFC 4103 text). See Emergency Access Advisory Committee (EAAC) Report on procedures for calls between TTY users and NG9-1-1 PSAPs [175] for further details.

© Copyright 2011-2022 National Emergency Number Association, Inc.

capabilities of the far end, as indicated by the value of the media feature tag returned by the far end in response to the SIP INVITE generated by the NIF. If, instead, a character other than space or line delimiter is received from the TTY user before the 1500 ms timer expires, then the NIF component will recognize that the " GA" was the beginning of a regular word, and reception of text from the TTY user will continue with no change of turn.

If a change of turn is in effect, and the media feature tag returned in a response to the initial SIP INVITE message generated by the NIF component has the value "text", the NIF SHALL substitute a line delimiter (e.g., CRLF) for the GA and forwards the line delimiter to the ESInet. The NIF SHALL then send any buffered characters received from the ESInet to the caller via the PIF and SHALL continue forwarding characters received from the ESInet in real time to the TTY caller using the mechanism described below.

If a change of turn is in effect, and the media feature tag received by the NIF component in a response to the initial SIP INVITE message has the value "urn:emergency:media-feature.tty-interworking", the NIF component SHALL pass the string of text characters (including the "GA") toward the PSAP, unchanged. As above, the NIF SHALL then send any buffered characters received from the ESInet to the caller via the PIF and SHALL continue forwarding characters received from the ESInet in real time to the TTY caller using the mechanism described below.

The NIF component MUST be capable of sending text characters toward a TTY caller, received from the ESInet toward a TTY caller. When the ESInet is sending text characters toward a TTY caller, the NIF will use the presence of a pre-defined pause between characters, or the presence of a " GA" or a line delimiter, to simulate a request by the PSAP to change the turn. Upon detecting a request to change the turn, the NIF component will add a "_GA" to the end of the text characters that are to be sent toward the caller, if "_GA" is not already present in the received text characters, as follows.

To support the interworking of RFC 4103 real-time text to Baudot tones performed by the PIF component of the Legacy Network Gateway, the NIF component SHALL initiate a provisionable inter-character timer, with a default value of 7 seconds, upon receipt of the first RFC 4103 text character from the ESInet. This timer SHALL be restarted with a value of 7 seconds every time a character is transmitted towards the TTY caller. If the characters "_GA" are detected, the inter-character timer shall be reduced to 1500 ms and if the NIF component receives no further text before the 1500 ms timer expires, the NIF component SHALL pass the text characters to the PIF component, unchanged. At this point, the turn will be changed and the NIF component will begin buffering any subsequent text from the ESInet. If additional text (other than a space or line delimiter) is received before the 1500 ms expires, the NIF component SHALL set the inter-character timer at 7 seconds and again continue forwarding characters toward the TTY caller and wait for a "_GA" or line delimiter.

© Copyright 2011-2022 National Emergency Number Association, Inc.

If a line delimiter is detected before the 7-second timer expires, the NIF component SHALL replace the line delimiter with a space and SHALL reset the inter-character timer to 1500 ms. If the inter-character timer expires without a "_GA" being detected, the NIF component SHALL append the characters "_GA" to the incoming RFC 4103 text and pass the text characters with the "_GA" appended to the PIF component for conversion to Baudot tones. At this point, a change of turn is performed, and the NIF component starts buffering characters received from the ESInet. If the NIF component receives a "_GA" before the 1500 ms timer expires, the NIF component SHALL follow the procedure described above for receipt of a "_GA". Once the inter-character timer has been initiated to 1500 ms, the receipt of space characters or line delimiters SHALL NOT cause the timer to be reset, rather the same procedure shall be followed as when the 1500 ms timer has expired.

The intention of the above procedure is to change turn and send "_GA" to the TTY caller when the PSAP sends a line delimiter or "_GA", possibly followed by spaces or line delimiters, but not immediately followed by text. A change of turn will also be made and "_GA" sent to the TTY caller when the PSAP is idle for an extended period of time, assuming that the PSAP makes no specific action to change turn. (A PSAP idle time of 7 seconds is specified in the Emergency Access Advisory Committee (EAAC) Report on procedures for the TTY as a text terminal in legacy 9-1-1 PSAPs without IP connection [175].) The NIF component will replace line delimiters used for text formatting (e.g., by i3 PSAPs) with a space because most TTYs have a limited display of only one or two lines. Such line delimiters SHALL NOT cause the NIF component to change turn. In addition, words beginning with "GA" should also not cause a change of turn. It is assumed that in such cases the next character in the word will be sent within the 1500 ms.

6.1.3 Location Interwork Function (LIF)

At the request of the NIF, the LIF SHALL invoke location retrieval functionality to obtain the location information that will be used as the basis for call routing and that will be delivered to the PSAP. Specifically, the LIF SHALL query an associated location server/database.

- If the call is a wireline emergency call, the associated database will contain location information in the form of a location value. This location value MAY be used for both routing and dispatch purposes.
- If the call is a Phase I wireless emergency call for which static caller location information is stored locally (i.e., no query is launched to the MPC/GMLC), the associated database will obtain a routing location by accessing pre-provisioned data that maps the ESRD to a routing location chosen so that it will route to the primary PSAP that is to receive the call, and MAY use the locally stored information as the caller's location for the call.

© Copyright 2011-2022 National Emergency Number Association, Inc.

- If the call is a wireless Phase II emergency call (or a Phase I wireless emergency call using this implementation), the associated database will access pre-provisioned data that maps the location key (i.e., ESRK or ESRD) provided with the call to a routing location chosen so that it will route to the target PSAP associated with the ESRK/ESRD, and will query an MPC/GMLC for caller location information.

The data in the internal location server/database are provisioned using proprietary mechanisms/interfaces, e.g., using the existing provisioning flows, systems, and interfaces that are used for provisioning legacy ALI databases today.

The LIF may receive one or two numbers/keys[65] from the NIF to be used for location retrieval/acquisition. Upon receiving the key(s), the LIF SHALL consult "steering" data to determine whether another system must be queried to obtain location information for dispatch purposes.

- If a single key is received from the NIF associated with a legacy wireline origination, it will not be present in the steering data. The LIF SHALL utilize internally defined procedures/protocols to retrieve static location information which SHALL be used for both routing and dispatch purposes from an associated location server/database.
- If the NIF provides two keys to the LIF and they are not present in the steering data (i.e., the keys include an ESRD that is associated with a Phase I wireless origination in which no MPC/GMLC query is to be launched), the LIF SHALL obtain routing location for the call by accessing pre-provisioned data in an associated database that maps the ESRD to a routing location chosen so that it will route to the target PSAP associated with the ESRD. Caller location will be retrieved from static location information accessed via internally defined procedures/protocols.
- If the key(s) include an ESRK or ESRD that is contained in the steering data, the LIF SHALL access pre-provisioned data in an associated database that maps the location key (i.e., ESRK or ESRD) to a routing location chosen so that it will route to the target PSAP associated with the ESRK/ESRD, and will generate an E2 ESPOSREQ message, as specified in J-STD-036-C-2 [50] or Mobile Location Protocol (MLP) query, as specified in Mobile Location Protocol 3.2 (RFC 7540) [197] (as appropriate for the MPC/GMLC whose address is included in the steering data) and direct it to the MPC/GMLC identified in the steering data to obtain the caller's location.

If the call is from a legacy wireline originating network, it is expected that the LIF will map the CPN/ANI to a location value (in the form of a civic address) and other non-location call-

[65] Note that in some networks, the callback number, when presented to the NIF, could be more than 10 digits when the caller number is international. Many networks truncate such numbers to 10 digits. The LNG MUST NOT truncate if the originating network can present more than 10 digits.

© Copyright 2011-2022 National Emergency Number Association, Inc.

related information (Refer to Appendix A for details on mapping between legacy and NG9-1-1 data). The location value and any non-location information will be returned to the NIF where it is used to build the corresponding Additional Data blocks.

If the call originated in a legacy wireless network using Wireline Compatibility Mode, the LIF SHALL interrogate its steering data with the ESRK. The steering data SHALL contain the address of the MPC/GMLC in the legacy wireless network that should be queried for initial/updated caller location. The LIF component SHALL obtain the routing location for the call by consulting an associated database that contains static mappings of ESRK to routing location chosen so that it will route to the target PSAP associated with the ESRK. The LIF component will also generate an E2 or MLP query for caller location, containing the ESRK, to the MPC/GMLC and MUST be capable of processing an E2/MLP response. The LIF component SHALL immediately return the routing location to the NIF component, along with an indication that the "Service Delivered by Provider to End User" is "wireless", and a SIP or HELD location reference that contains the ESRK and the URI of the Legacy Network Gateway. Upon receiving the caller location returned by the MPC/GMLC (which is initially expected to convey information about the location of the cell site/sector), the LIF component SHALL store the caller location and pass any non-location information received in the MPC/GMLC response, including the callback number, to the NIF component.

If the call originated in a legacy wireless network that supports the signaling of callback number and ESRD, the LIF component SHALL consult its steering data using the ESRD. The steering data includes the address of the MPC/GMLC in the legacy wireless network that should be queried for initial/updated caller location.

- If the legacy wireless network is only Phase-I-capable, the LIF may not find steering data that corresponds to the ESRD and will instead retrieve from its local database a static location value that is associated with the cell site/sector to be used as the caller location. The LIF SHALL obtain the routing location for the call by consulting an associated database that contains static mappings of ESRDs to routing location chosen so that it will route to the target PSAP associated with the ESRD. The LIF SHALL then pass the routing location, along with an indication that the "Service Delivered by Provider to End User" is "wireless", and originating network contact information (i.e., the "Data Provider Contact URI") to the NIF component. The LIF SHALL also pass a SIP or HELD location reference to the NIF that uniquely identifies the location information and the Legacy Network Gateway. The LIF will associate the location reference with the routing and caller location.
- If the LIF component finds steering data corresponding to the ESRD, it SHALL obtain the routing location for the call by consulting an associated database that contains static mappings of ESRD-to-routing-location chosen such that it will route to the target PSAP associated with the ESRD. The LIF component SHALL also generate an

© Copyright 2011-2022 National Emergency Number Association, Inc.

E2/MLP query for caller location, containing the callback number and ESRD, to the MPC/GMLC and MUST be capable of processing an E2/MLP response. The LIF component SHALL immediately return the routing location to the NIF component, along with an indication that the "Service Delivered by Provider to End User" is "wireless". The LIF SHALL also pass a SIP or HELD location reference to the NIF that uniquely identifies the location record and the Legacy Network Gateway**.** Upon receiving the caller location returned by the MPC/GMLC (which is initially expected to convey information about the location of the cell site/sector), the LIF component shall retain the caller location and associate it with the location reference**.** The LIF component will also pass any non-location information received in the E2/MLP response to the NIF component.

Since the Legacy Network Gateway may provide a location reference (e.g., associated with a legacy wireless emergency call origination) in the INVITE that it sends to the ESRP, the LIF MUST also support the dereferencing of location references by external elements (e.g., ESRPs, PSAPs). The interface used by a LIF for dereferencing is the same as the interface used by a LIS for dereferencing, as described in Section 3.2. Specifically, the LIF MUST support SIP and**/**or HELD dereferencing protocols and MUST be capable of applying the appropriate one based on the format of the location reference provided as output from the location retrieval process.

6.1.3.1 Interworking to Support Location Dereferencing

6.1.3.1.1 Interworking Between HELD and E2

The following tables illustrate the interworking between HELD and E2 to support location dereferencing.

Table 6-1 HELD locationRequest to E2 ESPOSREQ Mapping

HELD locationRequest→	ESPOSREQ→	Notes
locationURI	-	Reflects value provided in the Geolocation header field of the INVITE message sent by the LNG
locationType	-	May include the optional "exact" attribute and indicates "civic" and/or "geodetic"

© Copyright 2011-2022 National Emergency Number Association, Inc.

HELD locationRequest→	ESPOSREQ→	Notes
responseTime	Position Request Type	The HELD responseTime parameter indicates the purpose for which the location is being requested (i.e., "emergencyRouting" or "emergencyDispatch") and the amount of time the requesting entity is willing to wait for a response. Only HELD locationRequests with a responseTime of "emergencyDispatch" will be mapped to an E2 ESPOSREQ message, with a Position Request Type vaule set to "UPDATED or LAST KNOWN". If the wait time value in the responseTime attribute is set to 0 ms, the LNG SHALL return the most accurate location it has locally (e.g., Phase I or Phase II).
-	Package Type = Query With Permission	
-	Transaction ID	Assigned by the Legacy Network Gateway
-	Component Sequence	
-	Component Type = INVOKE (last)	
-	Component ID	Assigned by the Legacy Network Gateway
-	Operation Code = Emergency Services Position Request	
-	Parameter Set	
-	ESME Identification	Identifies the requesting entity
-	Emergency Services Routing Key	Populated with ESRK, if received by Legacy Network Gateway in incoming signaling from the MSC

© Copyright 2011-2022 National Emergency Number Association, Inc.

HELD locationRequest→	ESPOSREQ→	Notes
-	Callback Number - Request	Populated with callback number if received by Legacy Network Gateway in incoming signaling from the MSC
-	Emergency Services Routing Digits - Request	Populated with ESRD if received by Legacy Network Gateway in incoming signaling from the MSC

Table 6-2 E2 esposreq to HELD locationResponse Mapping

esposreq→	HELD locationResponse →	Notes
-	presence	Contains civic and/or geodetic location populated in a PIDF-LO; If the locationRequest contains a responseTime parameter value of "emergencyRouting," this parameter will be populated with the location mapped from the ESRK/ESRD, formatted as a PIDF-LO
Package Type = Response	-	
Transaction ID	-	
Component Sequence	-	
Component Type = Return Result (last)	-	
Component ID	-	
Parameter Set	-	
Position Result	-	Indicates whether returned position is initial, updated, last known, not available

© Copyright 2011-2022 National Emergency Number Association, Inc.

esposreq→	**HELD locationResponse →**	**Notes**
Position Information: - Generalized Time - Geographic Position - Position Source	presence	Indicates time of position determination One or the other of Position Information – Geographic Position or Location Description may be populated**, and when present,** MUST be populated with geodetic location and civic address, respectively. Both may be populated if both are available at the MPC. Geographic Position would map to geodetic location formatted as a PIDF-LO Method of location determination; Position Source maps to 'Method' parameter within PIDF-LO
Callback Number - Response	-	Populated with MDN/MSISDN that identifies the caller
Emergency Services Routing Digits - Response	-	Populated with the ESRD associated with the cell site/sector from which the emergency call originated
Mobile Identification Number	-	Optional
IMSI	-	Optional
Mobile Call Status	-	Optional
Company ID	-	Carries unique identifier for the Wireless Service Provider

© Copyright 2011-2022 National Emergency Number Association, Inc.

esposreq→	HELD locationResponse →	Notes
Location Description	presence	If present, the Location Description parameter will be used to populate a civic location in the PIDF-LO. The non-location information in this parameter will also be used by the LNG to create an Additional Data structure. See Appendix A for mappings of data elements received in Location Description Parameter to the PIDF-LO or Additional Data structure.

6.1.3.1.2 Interworking Between HELD and MLP

The following tables illustrate the interworking between HELD and MLP to support location dereferencing.

Table 6-3 HELD locationRequest to MLP ELIR Mapping

HELD locationRequest→	MLP ELIR→	Notes
locationURI	-	Reflects the value provided in the Geolocation header field of the INVITE message sent by the LNG
locationType	-	May include the optional "exact" attribute and indicates "civic" and/or "geodetic"
responseTime	Loc_Type	The HELD responseTime parameter indicates the purpose for which the location is being requested (i.e., "emergencyRouting" or "emergencyDispatch") and the amount of time the requesting entity is willing to wait for a response. Only HELD locationRequests with a responseTime of "emergencyDispatch" will be mapped to an MLP ELIR message, in which case the Loc_Type in the ELIR will be set to "CURRENT". If the wait time value in the responseTime attribute is set to 0 ms,

© Copyright 2011-2022 National Emergency Number Association, Inc.

HELD locationRequest→	MLP ELIR→	Notes
		the LNG SHALL return the most accurate location it has locally (e.g., Phase I or Phase II).
-	Header: - hdr ver=" 3.2.0" - client ○ id ○ pwd ○ serviceid	The *id* and *pwd* contain the username and password assigned by the WSP to the ILEC and is common to all ALIs within the redundant configuration. The *serviceid* may OPTIONALLY be used by the ILEC to identify the individual ALI making the request.
-	MSID = callback number	Two different types of MSID are possible: MSISDN or MDN; type used in ELIR will be appropriate for the ESRD
-	ESRD	
-	eqop - resp_timer[1]	Indicates the maximum time the MPC/GMLC has before it must respond to the request.
-	GEO_INFO	Defines the reference coordinate system (i.e., WGS 84)

[1]A value of 30 seconds is used in Canadian networks today.

Table 6-4 MLP ELIA to HELD locationResponse Mapping

MLP ELIA→	HELD locationResponse	Notes
-	presence	Contains civic and/or geodetic location populated in a PIDF-LO; If the locationRequest contains a responseTime parameter value of "emergencyRouting," this parameter will be populated with the location mapped from the ESRK/ESRD, formatted as a PIDF-LO
Result	-	Indicates whether or not an error occurred, and if so, what type of error

© Copyright 2011-2022 National Emergency Number Association, Inc.

MLP ELIA→	HELD locationResponse	Notes
EME_POS		
- MSID	-	From the ELIR message
- ESRD	-	From the ELIR message
- pd (Position Data)	presence	
○ time		Indicates time of position determination
○ shape		The shape returned in the ELIA message will be set to "Circular Area" with x and y coordinates and radius expressed in meters
○ lev_conf[2]		The percentage of confidence of the returned location This geo-location will be formatted as a PIDF-LO for population in the HELD locationResponse if the HELD locationRequest contains a responseTime parameter value of "emergencyDispatch"
pos_method[3]		Method of location determination; If present, pos_method maps to 'Method' parameter within PIDF-LO

[2]A value of 90% is used in Canadian networks today.

[3]This is an EME_POS attribute and is not provided in Canadian networks today.

6.1.3.1.3 Interworking Between SIP Presence and E2

Using SIP Presence with location by reference is discussed in Section 4.10. The following tables illustrate the interworking between SIP Presence and E2 to support location dereferencing.

© Copyright 2011-2022 National Emergency Number Association, Inc.

Table 6-5 SIP Presence SUBSCRIBE to E2 ESPOSREQ Mapping

SIP Subscribe→	ESPOSREQ→	Notes
location URI (in Request-URI and To:)	-	Reflects value provided in the Geolocation header field of the INVITE message sent by the LNG
Filter (in body)	-	MAY include rate filters and/or location filters
-	Position Request Type	Indicates whether initial or updated location is being requested; Initial NOTIFY contains the initial location, subsequent NOTIFYs contain updated location.
-	Package Type = Query With Permission	
-	Transaction ID	Assigned by the Legacy Network Gateway
-	Component Sequence	
-	Component Type = INVOKE (last)	
-	Component ID	Assigned by the Legacy Network Gateway
-	Operation Code = Emergency Services Position Request	
-	Parameter Set	
-	ESME Identification	Identifies the requesting entity
-	Emergency Services Routing Key	Populated with ESRK, if received by Legacy Network Gateway in incoming signaling from the MSC
-	Callback Number - Request	Populated with callback number if received by Legacy Network Gateway in incoming signaling from the MSC
-	Emergency Services Routing Digits - Request	Populated with ESRD if received by Legacy Network Gateway in incoming signaling from the MSC

© Copyright 2011-2022 National Emergency Number Association, Inc.

Table 6-6 E2 ESPOSREQ to SIP Presence NOTIFY Mapping

esposreq→	SIP NOTIFY→	Notes
-	presence	Contains civic and/or geodetic location populated in a PIDF-LO; Initial NOTIFY will contain ESRK/ESRD, formatted as a PIDF-LO
Package Type = Response	-	
Transaction ID	-	
Component Sequence	-	
Component Type = Return Result (last)	-	
Component ID	-	
Parameter Set	-	
Position Result	-	Indicates whether returned position is initial, updated, last known, not available
Position Information: - Generalized Time - Geographic Position 1. - Position Source	presence	Indicates time of position determination One or the other of Position Information – Geographic Position or Location Description may be populated**, and when present,** MUST be populated with geodetic location and civic address, respectively. Both may be populated if both are available at the MPC. Geographic Position would map to geodetic location formatted as a PIDF-LO Method of location determination: Position Source maps to 'Method' parameter within PIDF-LO
Callback Number - Response	-	Populated with MDN/MSISDN that identifies the caller
Emergency Services Routing Digits - Response	-	Populated with the ESRD associated with the cell site/sector from which the emergency call originated

© Copyright 2011-2022 National Emergency Number Association, Inc.

esposreq→	SIP NOTIFY→	Notes
Mobile Identification Number	-	Optional
IMSI	-	Optional
Mobile Call Status	-	Optional
Company ID	-	Carries unique identifier for the Wireless Service Provider
Location Description	presence	If present, the Location Description parameter SHALL be used to populate a civic location in the PIDF-LO. The non-location information in this parameter SHALL also be used by the LNG to create an Additional Data structure. See Appendix A for mappings of data elements received in Location Description Parameter to the PIDF-LO or Additional Data structure.

6.1.3.1.4 Interworking Between SIP Presence and MLP

The following tables illustrate the interworking between SIP Presence and MLP to support location dereferencing.

Table 6-7 SIP Presence SUBSCRIBE to MLP ELIR Mapping

SIP SUBSCRIBE→	MLP ELIR→	Notes
location URI (in Request-URI and To:)	-	Reflects value provided in the Geolocation header field of the INVITE message sent by the LNG
Filter (in body)	-	May include rate filters and/or location filters
-	Loc_Type	The SUBSCRIBE is mapped to an MLP ELIR message with Loc_Type set to "CURRENT"; Initial NOTIFY contains the most accurate location the LIF has locally at the time of subscription (i.e., Phase I or Phase II), the next NOTIFY contains the updated location.

© Copyright 2011-2022 National Emergency Number Association, Inc.

SIP SUBSCRIBE→	MLP ELIR→	Notes
-	Header: - hdr ver=" 3.2.0" - client ○ id ○ pwd ○ serviceid	The *id* and *pwd* contain the username and password assigned by the WSP to the ILEC and is common to all ALIs within the redundant configuration. The *serviceid* MAY optionally be used by the ILEC to identify the individual ALI making the request.
-	MSID = callback number	Two different types of MSID are possible: MSISDN or MDN; type used in ELIR will be appropriate for the ESRD
-	ESRD	
-	eqop - resp_timer[1]	Indicates the maximum time the MPC/GMLC has before it must respond to the request.
-	GEO_INFO	Defines the reference coordinate system (i.e., WGS 84)

[1]A value of 30 seconds is used in Canadian networks today.

Table 6-8 MLP ELIA to SIP Presence NOTIFY Mapping

MLP ELIA→	SIP NOTIFY→	Notes
-	presence	Contains civic and/or geodetic location populated in a PIDF-LO; If this is the first NOTIFY, this parameter SHALL be populated with the location mapped from the ESRK/ESRD, formatted as a PIDF-LO
Result	-	Indicates whether or not an error occurred, and if so, what type of error

© Copyright 2011-2022 National Emergency Number Association, Inc.

MLP ELIA→	SIP NOTIFY→	Notes
EME_POS		
- MSID	-	From the ELIR message
- ESRD	-	From the ELIR message
- pd (Position Data)	presence	
○ Time		Indicates time of position determination
○ Shape		The shape returned in the ELIA message will be set to "Circular Area" with x and y coordinates and radius expressed in meters
○ lev_conf[2]		The percentage of confidence of the returned location This geo-location SHALL be formatted as a PIDF-LO for population in the NOTIFY if this is not the first one.
pos_method[3]		Method of location determination; If present, pos_method maps to 'Method' parameter within PIDF-LO

[2]A value of 90% is used in Canadian networks today.

[3]This is an EME_POS attribute and is not provided in Canadian networks today.

6.1.3.2 Call Flow Example

Figure 6-2 illustrates a call flow in which a legacy wireless emergency call origination is routed via a Legacy Network Gateway to an ESRP in an i3 ESInet. This call flow assumes that the MSC delivers the call to the Legacy Network Gateway with an ESRK only. It also assumes that there is only one ESRP in the call path, and that HELD is used as the dereferencing protocol.

© Copyright 2011-2022 National Emergency Number Association, Inc.

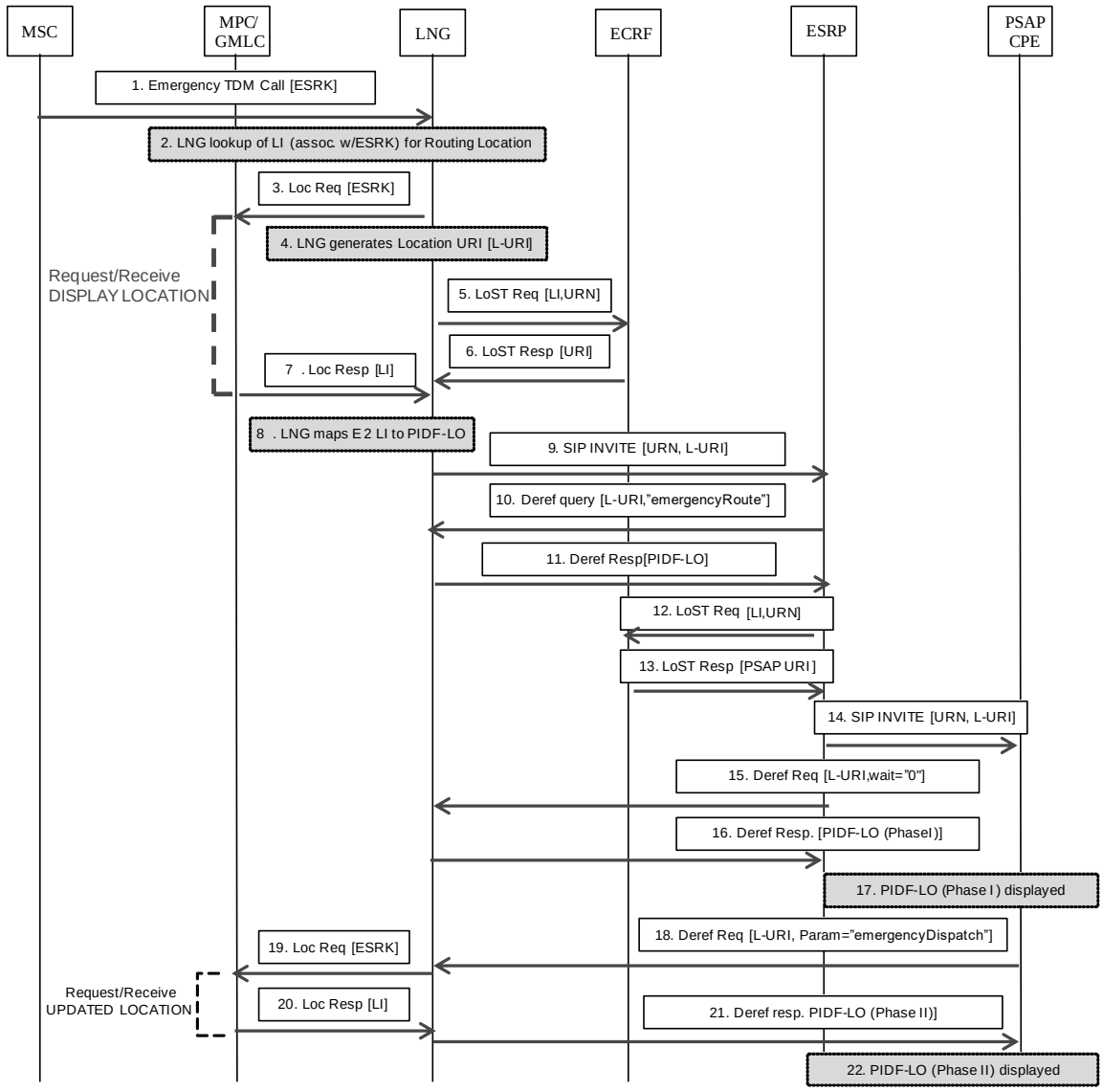


Figure 6-2 Example Call Flow

1. A legacy wireless emergency call origination is signaled from the MSC to the Legacy Network Gateway with an ESRK.
2. The Legacy Network Gateway maps the ESRK to a Routing Location (i.e., Location Information [LI]) that is chosen so that it will route to the PSAP that is associated with that ESRK.
3. The Legacy Network Gateway initiates a Location Request (e.g., an E2 ESPOSREQ) to the MPC/GMLC that contains the ESRK.

© Copyright 2011-2022 National Emergency Number Association, Inc.

4. The Legacy Network Gateway generates a location reference in the form of a HELD location URI. (Note that this can happen prior to Step 3.)
5. The Legacy Network Gateway sends a routing request to the ECRF that contains a service URN and the Routing Location (i.e., LI from Step 2).
6. The Legacy Network Gateway receives a routing response from the ECRF that contains the next hop ESRP URI.
7. Sometime after Step 3, the Legacy Network Gateway receives Phase I Location Information (Phase I LI) from the MPC/GMLC.
8. The Legacy Network Gateway maps the LI received from the MPC/GMLC to a PIDF-LO based on a mapping rule set (e.g., by accessing the MSAG Conversion Service [MCS]).
9. The Legacy Network Gateway forwards the SIP INVITE message to the ESRP (via a BCF which is not pictured). The INVITE message includes the location URI (from Step 4) in the Geolocation header field.
10. The ESRP sends a HELD dereference request to the Legacy Network Gateway. The HELD locationRequest includes the location URI and a responseTime parameter set to "emergencyRouting".
11. The Legacy Network Gateway returns the Routing Location to the ESRP formatted as a PIDF-LO.
12. The ESRP sends a routing request to the ECRF that contains a Service URN and the Routing Location.
13. The ESRP receives a routing response from the ECRF that contains a PSAP URI.
14. The ESRP forwards the SIP INVITE to the PSAP CPE. The INVITE contains the location URI from Step 4.
15. The PSAP CPE sends a HELD dereference request to the Legacy Network Gateway. The HELD locationRequest includes the location URI, and a responseTime parameter indicating a wait time of "0 ms". This tells the Legacy Network Gateway that it should return whatever location is currently available (i.e., the Phase I location received in Step 7).
16. The Legacy Network Gateway returns Phase I location information to the PSAP CPE, formatted as a PIDF-LO (from Step 8).
17. The Phase I location information is displayed at the PSAP CPE.
18. After waiting 30 seconds, the PSAP CPE sends an additional HELD dereference request to the Legacy Network Gateway. The HELD locationRequest includes the location URI, and a responseTime parameter set to "emergencyDispatch."
19. The Legacy Network Gateway sends a Location Request (i.e., E2 ESPOSREQ) to the MPC/GMLC, requesting updated/last known location. The Location Request includes the ESRK that was provided in call setup signaling from the MSC.
20. The MPC/GMLC returns updated/last known location (i.e., in an esposreq message).

© Copyright 2011-2022 National Emergency Number Association, Inc.

21. The Legacy Network Gateway returns the updated/last known Phase II location information to the PSAP, formatted as a PIDF-LO, in a HELD locationResponse message.
22. The Phase II location information is displayed at the PSAP CPE.

6.2 Legacy PSAP Gateway (LPG)

The Legacy PSAP Gateway is a signaling and media interconnection point between an ESInet and a legacy PSAP. It plays a role in the delivery of emergency calls that traverse an i3 ESInet to get to a legacy PSAP, as well as in the transfer and alternate routing of emergency calls between legacy PSAPs and i3 PSAPs. The Legacy PSAP Gateway supports an IP (i.e., SIP) interface towards the ESInet on one side, and a traditional MF or Enhanced MF interface (comparable to the interface between a traditional Selective Router (SR) and a legacy PSAP, described in NENA 03-002 [163]) on the other. The Legacy PSAP Gateway also includes an ALI interface (as defined in NENA-STA-027 [164] or NENA 04-005 [165]) that can accept an ALI query from the legacy PSAP. The legacy PSAP controller supplies an appropriate ALI query key (i.e., "ANI") for the call. When queried with this key, the Legacy PSAP Gateway responds with the location. If the emergency call routed via the ESInet contains a location by value, the Legacy PSAP Gateway responds with that value, formatted appropriately for the receiving PSAP. If the ESInet provides a location by reference, the ALI query to the Legacy PSAP Gateway results in a dereference operation from the gateway to the LIS or Legacy Network Gateway. The results of the dereference operation are returned to the Legacy PSAP Gateway, and subsequently passed from the Legacy PSAP Gateway to the legacy PSAP. The ALI response generated by the Legacy PSAP Gateway will also contain additional information that may be obtained from a variety of sources. See Section 6.2.2 for further discussion.

The Legacy PSAP Gateway functional element contains three functional components, as illustrated in Figure 6-1[66]:

1. (SIP-MF/E-MF/DTMF) Protocol Interwork Function (PIF). This functional component interworks the SIP protocol to traditional MF, Enhanced MF, or ISDN, or other

[66] Note that the functional decomposition of the Legacy PSAP Gateway described in this section is provided to assist the reader in understanding the functions and external interfaces that a Legacy PSAP Gateway must support. Actual implementations MAY distribute the functionality required of the Legacy PSAP Gateway differently among functional components, as long as all of the functions and external interfaces described herein are supported.

© Copyright 2011-2022 National Emergency Number Association, Inc.

protocols, as appropriate for the interconnected PSAP[67]. If the PIF component determines that the call is to be delivered to the PSAP as a TTY call, the PIF component will be responsible for interworking real-time text and TTY per RFC 5194 [84]. The PIF component MUST also be capable of interworking text messages received in an MSRP session with TTY. It is assumed that the PIF functional component does not require specialized hardware, and can therefore be implemented using commercially available hardware. (See Section 6.2.1 for further details.)

2. NG9-1-1-specific Interwork Function (NIF). This functional component provides NG9-1-1-specific processing of the call signaling, which includes special handling of attached location, selection of trunk groups, and callback number mapping, etc. The NIF associates one form of identifier with another, which includes mapping any combination of identifiers, such as 10-digit NANP numbers, non-NANP identifiers (pANIs), E.164 (International 11-15 digit) identifiers, and SIP URIs. For example, when a call is received with location and a SIP URI and it is destined for a legacy PSAP, the NIF maps the attached location and callback identifier information to a pANI that is then delivered to the PSAP with the call and used by the PSAP as a key for subsequent location and callback information retrieval. In addition, the NIF includes functionality to support transfer requests and, optionally, requests for the invocation of alternate routing (e.g., in cases of PSAP evacuation). This functional component should be viewed as a Back-to-Back User Agent (B2BUA) in front of the PIF. (See Section 6.2.2 for further details.)
3. Location Interwork Function (LIF). This functional component supports standard ALI query/response interface protocols, as well as the interworking of NG9-1-1 relevant data elements to a standardized ALI format for population in ALI response messages. (See Section 6.2.3 for further details.)

The LPG MUST implement the server-side of the ElementState event notification package.

The following subsections describe each of these functional components of the Legacy PSAP Gateway in detail.

Note: The LPG MUST log all significant events. Log record formats for this purpose are provided in Section 4.12.3 of this document.

[67] Note that only interworking between SIP and traditional MF, E-MF, and DTMF signaling are addressed in this specification. Interworking with ISDN and other protocols that may be used by legacy PSAPs is outside the scope of this specification.

© Copyright 2011-2022 National Emergency Number Association, Inc.

6.2.1 Protocol Interwork Function (PIF)

The PIF component of the Legacy PSAP Gateway will be responsible for interworking the SIP signaling received from the NIF component with the traditional or Enhanced MF signaling sent over the interface to the destination PSAP. The PIF will also be responsible for accepting Dual Tone Multi-Frequency (DTMF) signaling (e.g., associated with transfer requests) from the legacy PSAP and sending it to the NIF component in RTP packets, per RFC 4733 [142].

The PIF component of the Legacy PSAP Gateway MUST be capable of accepting a SIP INVITE message generated by the NIF component (see Section 6.2.2.3).

Upon receiving the INVITE method, the PIF component of the Legacy PSAP Gateway SHALL identify the destination PSAP based on the information in the Request-URI and select an outgoing trunk to that PSAP based on the outgoing trunk group information in the Request-URI. Based on the information received in incoming signaling from the NIF component, the PIF component SHALL generate either traditional MF (i.e., 8-digit CAMA) or Enhanced MF (E-MF) call signaling. In both cases, the MF signaling sequences used in delivering emergency calls to legacy PSAPs include a "Special Handling" indication along with the ANI[68]. (See Section 6.2.2.2 for further information.) Legacy PSAPs that support E-MF interfaces MAY support the delivery of a 10-digit key or pANI that serves as a reference to the caller's location information in addition to a 10-digit callback number and "Special Handling" indication. The traditional MF and E-MF signaling interfaces that may be supported by a legacy PSAP are described below.

6.2.1.1 Traditional MF Interface

If a traditional MF interface is supported by the legacy PSAP, the signaling interworking provided by the Legacy PSAP Gateway will be as depicted below:

[68] The "ANI" may contain the caller's callback information or a query key (i.e., a pANI).

© Copyright 2011-2022 National Emergency Number Association, Inc.

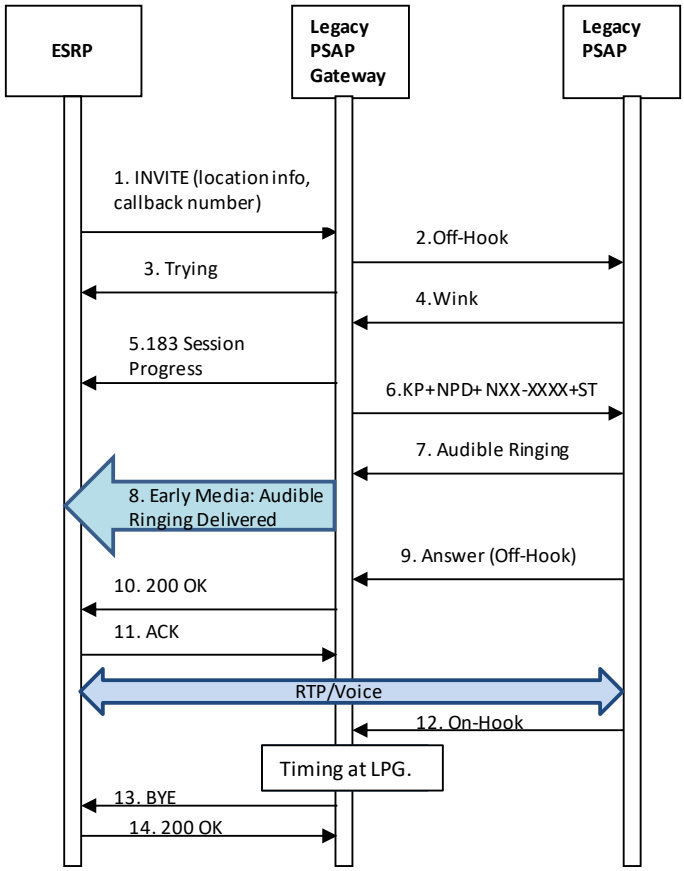


Figure 6-3 Call Delivery With Traditional MF Interface to PSAP

The emergency call delivery flow illustrated above begins when the ESRP determines that a call is to be delivered to a particular PSAP, and that the route to that PSAP is via the Legacy PSAP Gateway. Note that if this call was being delivered to the Legacy PSAP Gateway by a network that has implemented the Route All Calls Via a Conference Aware UA model, the ESRP in this call flow would be replaced by an ESRP/Conference Aware UA. This flow illustrates disconnect being initiated by the PSAP.

1. The ESRP constructs a SIP INVITE and sends it to the Legacy PSAP Gateway. The SIP INVITE is populated as described in RFC 3261 [10], with the clarifications provided in Sections 3.1 and 6.2.2.
2. When the NIF component of the Legacy PSAP Gateway receives the INVITE message, it follows the procedures described in RFC 3261 [10] for processing the INVITE, with the following clarifications. The NIF component of the Legacy PSAP Gateway uses the content of the INVITE to determine that the call is an emergency call, and to determine the information that will be signaled to the PSAP CPE to support such functions as display of ANI and queries for ALI information (i.e., the

© Copyright 2011-2022 National Emergency Number Association, Inc.

Numbering Plan Digit [NPD][69] and ANI digits to be signaled via MF to the legacy PSAP).

If the INVITE contains both callback information and location information, the NIF component SHALL be provisioned to determine, on a per-PSAP basis, whether the information signaled as the ANI will be associated with the callback information or the location information.

It is desirable that a callback number be delivered to the PSAP as the "ANI" for emergency calls that traverse an i3 ESInet, whenever possible. This will give the PSAP the ability to call back the emergency caller even if attempts to access ALI information are unsuccessful.

If, based on provisioning, the PSAP should receive callback information, the ANI will usually be based on the callback number/address included in the P-A-I (if available) or the From header field of the incoming INVITE message.

If the P-A-I or the From header field contains callback information that is in the form of a 10-digit NANP number, and the NPA portion of that number is appropriate for the target PSAP (i.e., can be associated with an appropriate NPD value), the NIF SHALL identify an NPD associated with the NPA and SHALL signal the NPD-NXX-XXXX in the From header field of the INVITE message sent to the PIF component. The PIF component SHALL then prepare to signal that NPD along with the NXX-XXXX portion of the callback number received in the incoming INVITE message in the ANI sequence.

If the P-A-I or the From header field in the INVITE message received by the NIF contains callback information that is either not in the form of a 10-digit NANP number, or is in the form of a 10-digit NANP number, but the NPA portion of that number is not appropriate for the target PSAP, the NIF SHALL identify an NPD associated with an NPA that is appropriate for the target PSAP, and SHALL generate locally a 7-digit pANI that consists of the following:

- An NXX of "511"
- An XXXX consisting of a sequential number from 0000 to 9999 with wrap around[70].

[69] See Section 6.2.2.2 for further discussion of NPD digits.

[70] Because the pANI is only sent by the Legacy PSAP Gateway to the legacy PSAP, and is not sent onward to any other entity, there is no significance beyond the gateway and the legacy PSAP.

© Copyright 2011-2022 National Emergency Number Association, Inc.

The NIF SHALL signal the pANI in the From header field of the INVITE message it sends to the PIF.

If, based on provisioning, the PSAP should only receive a location key, the NIF SHALL signal that information to the PIF in a From header field that consists of an NPD associated with an NPA that is appropriate for the target PSAP and a 7-digit pANI of the form 511-XXXX.

The PIF component of the Legacy Network Gateway creates connectivity (i.e., seizes an MF trunk) to the PSAP CPE for the emergency call.

3. After sending the INVITE message to the PIF component, the NIF component sends a SIP 100 Trying message to the ESRP. The PIF also sends a SIP 100 Trying message to the NIF component (not shown).
4. The PSAP CPE responds with a "wink" indicating that it is ready to receive further signaling related to the emergency call.

   If the PSAP fails to respond with a wink within four (4) seconds[71], the Legacy PSAP Gateway SHALL treat the call attempt as a failure, mark the PSAP trunk, and alert management personnel to the situation. If this is a first failure on the call, the Legacy PSAP Gateway SHALL make a second attempt on another PSAP trunk circuit or re-attempt on the same circuit after a sufficient guard time period to allow the PSAP trunk to idle itself in preparation for a subsequent call attempt. If the call failure is on a second attempt, the Legacy PSAP Gateway SHALL deem the call a failure, and return a SIP 500 Server Internal Error message to the NIF component, indicating that it was unable to present the call to the legacy PSAP. The NIF component SHALL signal the SIP 500 Server Internal Error message back to the ESRP. (See Section 6.2.4.1 for further information on call setup timing at the Legacy PSAP Gateway.)
5. The PIF component signals a SIP 183 Session Progress back to the NIF (not shown), and the NIF signals a SIP 183 Session Progress message back to the ESRP, indicating that connectivity should be established in the backward direction to support call progress signaling (i.e., early media/audible ringing) provided by PSAP CPE. The Contact header field in the SIP 183 Session Progress message sent by the NIF to the ESRP shall include a "text" media feature tag.
6. The PIF signals an MF digit string consisting of a Key Pulse (KP) signal followed by the NPD and seven NXX-XXXX digits derived in Step 2. The MF signaling sequence

[71] The 4-second timer is specified in ATIS-0600414.1998(R2007), *Network to Customer Installation Interfaces – Enhanced 911 Analog Voicegrade PSAP Access Using Loop Reverse-Battery Signaling*. [188]

© Copyright 2011-2022 National Emergency Number Association, Inc.

ends with the Start (ST) signal. (See GR-350-CORE [189] or NENA-STA-027 [164] for further discussion of signaling sequences associated with traditional MF interfaces.)

7. Upon receiving complete ANI information, the PSAP signals the attendant and returns audible ringing to the calling party.
8. Early media/audible ringing is delivered via the ESRP to the calling UA.
9. The PSAP call taker answers the call and the off-hook signal is conveyed to the PIF.
10. The PIF component sends a SIP 200 OK message to the NIF component (not shown) and the NIF component sends a SIP 200 OK message to the ESRP.
11. The ESRP forwards the SIP ACK generated by the calling UA to the NIF component of the Legacy PSAP Gateway to confirm acceptance of the answer indication. The NIF component forwards the SIP ACK to the PIF component (not shown).

The media streams are established. The caller and the PSAP call taker can now communicate.

12. In this example flow, the PSAP initiates the release of the call by sending an on-hook signal to the Legacy PSAP Gateway.

    The Legacy PSAP Gateway MUST determine if the on-hook condition is a true disconnect (i.e., the on-hook condition persists for >1100ms), or a hook flash (500ms +/- 250ms). Therefore, in this example, where the PSAP disconnects first, there will be a timing interval between the on-hook signal from the PSAP, and the SIP BYE message being sent (in Step 13). It is RECOMMENDED that this interval be a minimum of 1100ms. See Section 6.2.4.2 for further information about call disconnect timing.

13. In response to receiving the on-hook signal from the legacy PSAP CPE, the PIF component sends a SIP BYE message to the NIF (not shown) and the NIF component sends a BYE message to the ESRP.
14. The ESRP forwards the 200 OK message generated by the calling UA, confirming the call termination.

6.2.1.2 Enhanced MF (E-MF) Interface

As described in Section 6.2.2.3, the use of E-MF signaling on an interface to a legacy PSAP will be selectable on a trunk group basis by the Legacy PSAP Gateway. A legacy PSAP that supports an E-MF interface may be capable of receiving one or two MF signaling sequences. If a PSAP supports the delivery of only one 10-digit number, and only the callback number, referred to in E-MF as the Calling Station Number, is available, the PIF component of the Legacy PSAP Gateway SHALL signal the following:

KP + II + NPA NXX XXXX ST',

© Copyright 2011-2022 National Emergency Number Association, Inc.

where NPA NXX XXXX is the Calling Station Number obtained from the From header field of the incoming INVITE message sent by the NIF and the ST' denotes the omission of the second 10-digit number sequence. The value to be signaled forward in the II digits will be obtained from the oli parameter in the From header field of the INVITE message from the NIF. (See Section 6.2.2.2 for further discussion of encoding of the II digits.) Today, this scenario is typically associated with the delivery of wireline emergency calls to legacy PSAPs.

When the PSAP supports delivery of two 10-digit numbers via the E-MF interface, the PIF component of the Legacy PSAP Gateway shall signal the following:

KP + II + NPA NXX XXXX ST KP NPA NXX XXXX ST

where the first NPA NXX XXXX is the callback/Calling Station Number received in the P-A-I header field of the INVITE from the NIF and the second NPA NXX XXXX contains a location key/reference formatted as a 10-digit NANP number obtained from the From header field of the INVITE message from the NIF. The value to be signaled forward in the II digits will be obtained from the oli parameter in the P-A-I header field of the INVITE message from the NIF. (See Section 6.2.2.2 for further discussion of the encoding of the II digits.)[72] Today, this scenario is typically associated with the delivery of wireless emergency calls to legacy PSAPs.

With respect to emergency call originations routed via a legacy Emergency Services Network, if a PSAP is capable of receiving only one 10-digit number, and both the callback number/Calling Station Number and location reference are available at the SR, the SR is provisioned to determine, on a per-PSAP basis, whether to signal the Calling Station Number or the location reference. For VoIP emergency call originations routed via an ESInet/NGCS, if the PSAP is only capable of receiving one 10-digit number, and both callback information and location information are received by the Legacy PSAP Gateway in the incoming INVITE, the NIF component of the Legacy PSAP Gateway SHALL determine, on a per-PSAP basis, whether to signal the callback information or location information to the legacy PSAP. In either case the PIF component of the Legacy PSAP Gateway shall signal the following:

KP + II + NPA NXX XXXX + ST'

where NPA NXX XXXX is the one 10-digit number specified by the PSAP and provided in the From header field of the incoming INVITE message from the NIF. The II value to signal

[72] See GR-2953-CORE [190] or NENA 03-002 [163] for further discussion of MF signaling sequences associated with E-MF interfaces.

© Copyright 2011-2022 National Emergency Number Association, Inc.

forward will be determined based on the information in the oli parameter in the From header field of the received INVITE message.

(See Section 6.2.2.2 for a discussion of the encoding of the II digits under the above scenarios.)

The call flow for a legacy PSAP that utilizes an E-MF interface is the same as that depicted in Figure 6-2 for a PSAP that utilizes a traditional MF interface, with the following modifications:

- In Step 3, the NIF component of the Legacy PSAP Gateway will determine, via provisioning, whether one or two 10 digit numbers are to be signaled to the destination PSAP, and will populate that information accordingly in the INVITE message it sends to the PIF (see Section 6.2.2.3.1). The PIF will determine the information to be populated in that/those signaling sequence(s) based on the information received in the INVITE from the NIF.

  If, based on provisioning, the PSAP is supposed to receive two 10-digit numbers, the NIF will include a P-A-I header field containing callback information and a From header field containing location information in the INVITE message it sends to the PIF. The PIF will use the callback information in the P-A-I to populate the first MF sequence, and the location key/reference from the From header field to populate the second MF sequence.

  The PIF will populate the II digits based on the oli parameter in the P-A-I header field of the INVITE from the NIF.

  If, based on provisioning, the PSAP is supposed to receive only a single 10-digit number, the NIF will populate the associated information in the From header field of the INVITE message it sends to the PIF. The PIF will take the information from the From header field of the received INVITE to populate the single outgoing MF sequence. The PIF will populate the II digits based on the oli parameter in the From header field of the INVITE from the NIF**.**
- In Step 6, the signaling sequence generated by the PIF SHALL either consist of KP + II + NPA NXX XXXX ST' or KP + II + NPA NXX XXXX ST KP NPA NXX XXXX ST. If the PIF only receives a From header field in the INVITE message from the NIF, it SHALL populate the MF signaling sequence KP + NPA NXX XXXX + ST' based on this information. If the PIF receives both a From header field and a P-A-I header field in the INVITE message from the NIF, it SHALL populate the first MF sequence based on the content of the P-A-I header field, and the second MF sequence based on the content of the From header field.

© Copyright 2011-2022 National Emergency Number Association, Inc.

If the PIF receives a From header field and no P-A-I header field in the INVITE message from the NIF, it SHALL populate the II digits based on the oli parameter in the From header field. If the PIF receives both a From header field and a P-A-I header field in the INVITE message from the NIF, it SHALL populate the II digits based on the oli parameter in the P-A-I header field.

6.2.1.3 Handling of Media Associated with TTY Calls

If an incoming call is to be delivered by the Legacy PSAP Gateway to the PSAP as a TTY call, the PIF component will be responsible for recognizing the media format provided in the SDP as being associated with real-time text and generating Baudot tones for delivery to the legacy PSAP.

If a legacy PSAP responds to an incoming call by generating Baudot tones, the PIF component SHALL be responsible for recognizing the Baudot tones in incoming media and replacing them with RFC 4103 [85] real-time text.

If an emergency call is presented to the PSAP as a "silent" call, (causing the PSAP to generate Baudot tones toward the caller), the PIF component of the Legacy PSAP Gateway MUST be capable of generating a re-INVITE message (upon receipt of the Baudot tones from the PSAP) and sending it to the NIF component to request the establishment of a real-time text media session over which the RFC 4013 [85] real-time text (which the PIF component transcodes from the incoming Baudot tones) can be sent. The PIF component SHALL buffer any real-time text that is converted from the received Baudot tones until such time as the text media session is established (i.e., until a 200 OK message is received from the NIF component in response to the re-INVITE) and the real-time text can be passed forward. The re-INVITE message generated by the PIF component of the Legacy PSAP Gateway SHALL include the following information:

- A Request-URI that contains a URI populated based on the content of the Contact header field received in the initial INVITE message.
    - If the initial emergency call was routed to the LPG via a network that has implemented the transfer procedures described in Section 4.7.1.1, the Request-URI SHALL contain a URI that is associated with the Legacy Network Gateway or caller.
    - If the initial emergency call was routed to the LPG via a network that has implemented the transfer procedures described in Section 4.7.1.2, the Request-URI SHALL contain a URI that is associated with the B2BUA.
    - If the initial emergency call was routed to the LPG via network that has implemented the Route All Calls Via a Conference Aware UA model (see Section 4.7.1.3), the Request-URI SHALL contain a URI that is associated with the Conference Aware UA.

© Copyright 2011-2022 National Emergency Number Association, Inc.

- A To header field that contains the information delivered to the Legacy PSAP Gateway in the From header field of the original INVITE message.
- A From header field that contains the digits "911" expressed as a URI (received in the To header field of the original INVITE message).
- A Contact header field that contains the content of the Request-URI provided in the initial INVITE message (i.e., a PSAP URI resolving at the gateway expressed as a tel URI or a sip URI of the form "sip:<TN>@psap1.gateway.com;user=phone", along with the trunk group parameters that identify the outgoing trunk group to the destination PSAP.
- A Via header field that is populated with a URI associated with the Legacy PSAP Gateway.
- An SDP offer that includes a media format associated with real-time text, as described in RFC 4103 [85].

Upon receiving the re-INVITE message from the PIF component, the NIF component SHALL pass the re-INVITE message toward the caller/Legacy Network Gateway/ingress LSRG, as described in Section 6.2.2.4. When the NIF component receives a 200 OK message indicating that the SDP offer associated with real-time text has been accepted, it SHALL pass the 200 OK message to the PIF component. The PIF component SHALL respond by sending an ACK to the NIF component, and the NIF component SHALL send an ACK toward the caller/Legacy Network Gateway/ingress LSRG.

6.2.1.4 Handling of Media Associated with SMS/MMS[73], Instant Messaging and RTT

Interworking of SMS/MMS and Instant Messaging (IM) to MSRP is expected to occur outside the ESInet, but Legacy PSAPs MUST have the capability to accept SMS/MMS/IM text messages that are interworked from MSRP to TTY. Interworking between MSRP and TTY MUST occur within the LPG. The LPG MUST also be capable of receiving RTT RTP packets and interworking them to TTY (Baudot tones) for delivery to legacy PSAPs. RFC 4103 describes a mechanism for carrying real-time text conversation session contents in RTP packets, but provides little guidance for handling the "turn-taking" that is inherent in interworking with TTY devices. There are currently no industry standards that describe this critical aspect of interworking with TTY. The FCC EAAC Report on "Proposed procedures for the TTY as a text terminal in legacy 9-1-1 PSAPs without IP connection" [175] provides some recommendations for the use of TTY terminals in legacy 9-1-1 PSAPs as text

[73] As specified in ATIS J-STD-110.v002 [191], only the text portion of an MMS origination is presented to the ESInet.

© Copyright 2011-2022 National Emergency Number Association, Inc.

terminals that can support more modern forms of text communication. In this context, the EAAC Report provides guidance related to the interworking of TTY with RTT and MSRP.

To support RTT, the PIF MUST interwork the RFC 4103 real-time text forwarded by the NIF to Baudot tones and MUST interwork Baudot tones generated by a legacy PSAP to RTT RTP packets and pass them toward the caller via the NIF component. There are also considerations for this interworking related to collision control and character mapping.

TTY can transmit in one direction at a time (half-duplex) and has created a need for strict "turn-taking" procedures. In the legacy environment, these procedures are adhered to by the users at each end. However, when a network element (e.g., an LPG) interworks between IP and TTY, that network element MUST emulate these procedures. This is also true given that the caller is unaware that his/her text session is being interworked to TTY and as such cannot be expected to abide by the turn-taking procedures dictated by TTY. The NIF component of the Legacy PSAP Gateway is responsible for facilitating the "turn-taking" expected by the TTY users involved in the conversation. (See Section 6.2.2.5 for further details.)

When the PIF component receives RFC 4103 real-time text packet from the NIF component over an established text media stream, the PIF component SHALL interwork the text characters to Baudot tones.

RFC 4103 states that "…common mean character transmission rate, during a complete PSTN text telephony session, is around two characters per second". It also states, "A maximum performance of 20 characters per second is enough even for voice-to-text applications." The EACC Report states, "TTY transmission is only at a speed of around 5 characters per second." This standard RECOMMENDS that the five (5) character per second guideline for transmission rate be followed. If RTT packets are received by the PIF component faster than the TTY transmission rate, they MUST be buffered.

TTY also restricts the character sets that can be used. The PIF component SHALL apply the following character mapping as defined in the EAAC Report [175] when translating from RFC 4103 text to TTY.

- During transmission, the PIF component SHALL check every character for validity in the TTY character set.
- The PIF component shall convert upper case to lower case
- The PIF component SHALL support the following translation of the special characters that have no representation in TTY:

RTT	TTY
At sign character "@"	Replace with "(at)"
Octothorpe or hash sign character "#"	Replace with dollar sign character "$"

© Copyright 2011-2022 National Emergency Number Association, Inc.

RTT	TTY
Percentage character "%"	Replace with slash character "/"
Ampersand character "&"	Replace with plus sign character "+"
Asterisk character "*"	Replace with a period character "."
Underscore character "_"	Replace with space character " "
Less than sign character "<"	Replace with left parenthesis character "("
Greater than sign character ">"	Replace with right parenthesis character ")"
National character	Replace with the closest companion in the a-z character range (e.g., "ñ" => "n")
Unknown character[74]	Replace with apostrophe character '

- The PIF component shall convert to 5-bit code and add shift character if needed.
- The PIF component SHALL transmit according to TIA 825A [183].

If the PIF component receives simultaneous RTT text and audio media associated with an emergency call (or one media type is added to an existing session involving the other media type), and since the audio media may include Baudot tones or other audio sounds, the PIF component MUST notch the audio frequencies used for Baudot tones from the received audio media and then insert the Baudot tones transcoded from the received RFC 4103 text to minimize the distortion of the Baudot tones delivered to the PSAP.

If a caller requests the use of Hearing Carry Over (HCO) or Voice Carry Over (VCO), the PSAP may need to switch between voice and TTY on a single call. The PIF component SHALL map voice received from the PSAP into RTP voice and Baudot tones received from the PSAP into RFC 4103 text.

SMS/MMS/IM text to 9-1-1 messages are delivered to the LPG using MSRP. MSRP messages are sent in "session mode" in which the entire message is sent. The NIF component is responsible for caching the MSRP message and converting it to RFC 4103 real-time text for delivery to the PIF component. The PIF component of the LPG MUST convert the RFC 4103 text to TTY for delivery to a legacy PSAP. As for the RTT case, the NIF component SHALL be responsible for maintaining the conventions associated with TTY calling (See Section 6.2.2.5). Upon determining that the call taker has joined the conversation (via receipt of an appropriate preprogrammed or typed message such as "911 GA"), the PIF component of the LPG SHALL convert the Baudot to RFC 4103 text characters and send the text characters to the NIF component.

[74] Other characters not in the TTY character set

© Copyright 2011-2022 National Emergency Number Association, Inc.

With respect to incoming RFC 4103 text characters received from the NIF component, the PIF component SHALL apply the same mapping to the text characters as described above for an RTT message when interworking with Baudot tones sent to the legacy PSAP.

The five (5) character-per-second EACC guideline SHOULD be followed in mapping the RFC 4103 text characters associated with an MSRP message to TTY.

6.2.1.5 Handling of Video Media

A Legacy PSAP is unable to handle video, and the PIF will not return an SDP media line for any video offer. Only the audio media will pass through to the PSAP.

6.2.2 NG9-1-1-Specific Interwork Function (NIF)

The NIF component of the Legacy PSAP Gateway functional element is expected to provide special processing of the information received in incoming call setup signaling to facilitate call delivery to legacy PSAPs, to assist legacy PSAPs in obtaining the necessary callback and location information, and to support feature functionality currently available to legacy PSAPs, such as call transfer and requests for alternate routing.

The NIF component of the Legacy PSAP Gateway MUST be capable of accepting SIP signaling associated with emergency call originations, as described in Section 3.1. Specifically, the NIF component of the Legacy PSAP Gateway MUST be capable of receiving and processing an INVITE that includes the following information:

- Request-URI = urn:service:sos
- Max Forwards <70
- Record Route = ESRP URI (this URI should contain the "lr" parameter to avoid Request-URI rewriting)
- Route header field = PSAP URI (this URI should contain the "lr" parameter to avoid Request-URI rewriting) resolving at the gateway[75]
- From = Callback Number/Address or "Anonymous," if unavailable
- To: (e.g., sip:911@vsp.com)
- P-A-I = the callback number/address or omitted if call is from a non-initialized mobile caller (i.e., P-Preferred-Identity containing 911 + "last 7 digits of the ESN or IMEI expressed as a decimal" is present)

[75] A Legacy PSAP Gateway could support more than one legacy PSAP. Each legacy PSAP would have a separate URI, but they would all resolve to the gateway. As an example, the PSAP URI for PSAP "A" might be "psapA@gateway1.esinet.net;lr" and the PSAP URI for PSAP "B" might be "psapB@gateway1.esinet.net;lr". The domain of the gateway in this example would be "gateway1.esinet.net".

© Copyright 2011-2022 National Emergency Number Association, Inc.

- P-Preferred-Identity = 911 + "last 7 digits of the ESN or IMEI expressed as a decimal" (if present for emergency calls originated by non-initialized mobile callers)
- Via = ESRP URI (added to other Via header fields present in the INVITE message received by the terminating ESRP)
- Contact = one of the following, depending on the transfer model implemented, and includes either a "text" media feature tag or a "urn:emergency:media-feature.tty-interworking" media feature tag
    - a SIP URI or tel URI identifying the user to facilitate an immediate callback to the device that placed the emergency call, or a SIP URI associated with a Legacy Network Gateway, if the RFC 4579-based [39] transfer model described in Section 4.7.1.1 is implemented
    - a SIP URI associated with a B2BUA, if the transfer model described in Section 4.7.1.2 is implemented
    - a SIP URI that is associated with the Conference Aware UA, if the transfer model described in Section 4.8.3 is implemented
- Supported = as received by the terminating ESRP
- SDP = as received by the terminating ESRP
- Geolocation = Content Identifier URI or location reference URI
- A Geolocation-Routing header field set to "yes"
- Call-Info = a URI which, when de-referenced, would yield additional information about the call or a cid: URI that points to additional information populated in the message body
- History-Info = as specified in RFC 7044 [35], with a Reason Parameter (as received in the incoming INVITE from the ESRPs)

Upon receiving an INVITE message from an ESRP, the NIF component SHALL analyze the signaled information and apply NG9-1-1-specific processing to ensure that the information delivered to the PSAP is in an acceptable format.

6.2.2.1 Handling of Emergency Calls with Non-NANP Callback Information

Traditional MF and E-MF interfaces to legacy PSAPs assume that callback information signaled to a PSAP will be in the form of a 7/10 digit NANP number. There are specific non-NANP number strings defined for use in scenarios in which the callback number is either missing or garbled. It is possible that VoIP or legacy wireless emergency call originations will contain callback information that is not in the form of (or easily converted to) a 10 digit NANP number. To address this situation, the NIF component of the Legacy PSAP Gateway SHALL perform a mapping from the non-NANP callback information to a locally significant digit string that can be delivered to the legacy PSAP via traditional MF or E-MF signaling. As described in Sections 6.2.1.1 and 6.2.1.2, the locally significant digit string delivered to the PSAP SHALL be of the form "NPD/NPA-511-XXXX". If a pANI of the form

© Copyright 2011-2022 National Emergency Number Association, Inc.

NPD/NPA-511-XXXX is sent in the MF sequence corresponding to the callback number, the same digit string can be generated by the Legacy PSAP Gateway and delivered to the legacy PSAP as a pANI that represents location information received by the Legacy PSAP Gateway in incoming signaling.

Note that legacy PSAPs will not be able to initiate a callback if the callback information associated with the emergency call is not in the form of an NANP number.

6.2.2.2 Special Handling Indication

Whether a legacy PSAP supports a traditional MF interface or an E-MF interface, it is possible for the information that appears at the PSAP CPE display to "flash" if the call has first been default-routed or alternate-routed. Today, in a legacy E9-1-1 environment, the decision about whether or not to flash the display at the PSAP depends upon local administration of Emergency Services Number (ESN) information.

In a legacy E9-1-1 environment, default routing occurs when the initial selective routing process at the first SR fails, due to a valid ESN not being produced, or no valid Calling Station Information being available on a wireline call, or no valid cell site and sector information being available on a wireless call. Under these circumstances, the call is sent to the default ESN associated with the incoming trunk group for that call.

Alternate routing occurs when the interface to a selected PSAP is found to be busy for any of these conditions: traffic busy (all trunks in use), night transfer (make-busy key operated), or upon detection of a failure condition (all trunks out of service). The alternate PSAP (or other destination) to which the call is routed may be on the same SR as the first PSAP or it may be served by a different SR.

In a legacy environment, whether flashing will occur depends upon the particular ESN used to point the call to the PSAP. Each SR has a list of ESNs that indicate that flashing should occur when calls are directed to the associated PSAP. ESN definitions are under local control. An incoming call could be mapped to a flashing ESN at one SR, and the same call could be mapped to a non-flashing ESN at the second SR.

An SR indicates to the PSAP CPE that a flashing display should be provided by the NPD value or the "II" value signaled to the legacy PSAP in the MF signaling sequence. For PSAPs that support traditional MF interfaces, an NPD digit with a value of 0-3 represents a steady ANI display. An NPD digit with a value of 4-7 represents a flashing ANI display (An NPD value of "8" is used for test calls). For PSAPs that support an E-MF interface, an II value of "40" indicates a steady display, and a value of "44" represents a flashing display. (An II value of "48" is used for test calls.)

One other scenario in which the II digits are used to communicate "special handling" is when a PSAP supports the delivery of a single 10-digit number over an E-MF interface and

© Copyright 2011-2022 National Emergency Number Association, Inc.

expects the Calling Station Number to be delivered, but a 10-digit location reference is signaled instead because the Calling Station Number is not available.

In the current i3 architecture, the ESRP interacts with a PRF to identify alternate routing addresses based on policy information associated with the next hop in the signaling path. The i3 Solution must support a means of signaling forward an indication that alternate/default routing has been applied to an emergency call so that the Legacy PSAP Gateway can determine when to include a Special Handling Indication in the MF signaling it sends to the legacy PSAP[76]. The ESRP shall use the History-Info header field (RFC 7044 [35]) and a Reason header field to communicate an indication of alternate/default routing. The NIF component of the Legacy PSAP Gateway will determine the appropriate coding of the NPD or II based on the content of received History-Info and Reason header fields and provisioning associated with the destination PSAP.

6.2.2.3 Internal Interface to the PIF Component

The NIF component SHALL generate an INVITE message to be sent to the PIF component. This message SHALL contain information from the incoming INVITE message associated with the emergency call, as well as any pANIs mapped by the NIF component. The NIF MUST determine, based on provisioning, whether the interface to the target PSAP is a traditional or Enhanced MF interface so that it can populate the callback and location information correctly in the INVITE that it sends to the PIF component. The NIF SHALL obtain callback information from the incoming INVITE message in the following way. If the incoming INVITE message contains a P-A-I header field, it will use the information in this header field as callback information. If the incoming INVITE message does not contain a P-A-I header field, the NIF will look in the From header field. If the From header field contains a value other than "Anonymous", the NIF will use the content of the From header field as the callback information. If the From header field contains the value "Anonymous" and a P-Preferred-Identity header field is present in the message, the NIF will use the content of the P-Preferred-Identity as the callback information. The NIF will obtain location information from the Geolocation header field of the incoming INVITE message.

If the PSAP supports a traditional MF interface, then the NIF SHALL determine, based on provisioning associated with the destination PSAP, whether to populate the From header field of the INVITE message that it sends to the PIF with an NPD + 7-digit number that is

[76] It is not currently assumed that a Legacy PSAP Gateway will have the intelligence to autonomously determine (e.g., via provisioning) an alternate PSAP based on detection of a busy or failure condition on the trunk to the primary PSAP.

© Copyright 2011-2022 National Emergency Number Association, Inc.

associated with callback information or with an NPD + 7-digit number that is associated with the location information.

If the PSAP expects callback information to be delivered, but the callback information is unavailable or is of the form 911+ "last 7 digits of the ESN or IMEI expressed as a decimal", and location information is available, the NIF SHOULD signal the location information in the From header field. If the PSAP expects location information to be delivered and location information is not available, or if neither callback information nor location information is available, the digits "0-9-1-1-0000" SHALL be signaled in the From header field.

A legacy PSAP that supports an E-MF interface may be capable of receiving one or two MF signaling sequences. If a PSAP supports the delivery of only one 10-digit number, the NIF SHALL determine, based on per-PSAP provisioning, whether callback information or location information should be populated in the From header field of the INVITE message it sends to the PIF. If the expected 10-digit number (e.g., Calling Station Number) is unavailable, but the second number (e.g., corresponding to the caller's location) is available, the available 10-digit number SHOULD be signaled in the From header field. If neither 10-digit number is available, and only one 10-digit number is expected to be signaled over the E-MF interface, the digits "000-911-0000" SHALL be signaled in the From header field.

If the legacy PSAP supports an E-MF interface and is capable of receiving two MF signaling sequences, the NIF SHALL populate a 10-digit number that represents location in the From header field and a 10-digit number that represents callback information in the P-A-I header field of the INVITE it sends to the PIF.

If the legacy PSAP supports an Enhanced MF interface in which two 10-digit sequences are expected, and either the Calling Station Number or the location reference is unavailable, the NIF SHOULD substitute the digits "000-911-0000" for the missing information in the P-A-I or From header field. If neither 10-digit number is available, and two 10-digit numbers are expected to be signaled over E-MF interface, the NIF SHALL substitute the digits "000-911-0000" for both the Calling Station Number and the location reference.

6.2.2.3.1 INVITE Message Sent from NIF Component to PIF Component

The INVITE message sent by the NIF component to the PIF component SHALL contain the following information:

- Request-URI = PSAP URI resolving at the gateway expressed as a tel URI or a sip URI of the form "sip:<TN>@psap1.gateway.com;user=phone", along with the trunk group parameters that identify the outgoing trunk group to the destination PSAP, as defined in RFC 4904.

© Copyright 2011-2022 National Emergency Number Association, Inc.

- Max Forwards <70
- Record-Route = ESRP URI, if presenting the SIP INVITE received from the ESRP
- From = See Table 6-9
- To = sip:911@vsp.com
- P-A-I = See Table 6-9
- Via = an identifier for the Legacy PSAP Gateway
- Contact = as received by the NIF component
- Supported = as received by the NIF component
- SDP = as received by the NIF component
- History-Info = as received (if present in the INVITE message received by the NIF component
- Reason = as received (if present in the INVITE message received by the NIF component.

Table 6-9 Population of From and P-A-I Header fields in INVITE Message Sent to PIF

PSAP Interface Supported	Scenario	From Header field Content	P-A-I Header field Content
Traditional MF	Callback information expected and available	NPD-NXX-XXXX or NPD-511-XXXX (associated with callback information)	Not present
Traditional MF	Location information expected and available	NPD-511-XXXX (associated with location information)	Not present
Traditional MF	Callback information desired; only location information available or non-initialized mobile caller	NPD-511-XXXX (associated with location information)	Not present
Traditional MF	Location information desired; only callback information available	0-911-0000	Not present
Traditional MF	Neither callback nor location available	0-911-0000	Not present

© Copyright 2011-2022 National Emergency Number Association, Inc.

PSAP Interface Supported	Scenario	From Header field Content	P-A-I Header field Content
Enhanced MF	Interface supports delivery of 20 digits; callback and location information are available	NPA-511-XXXX (associated with location information)	NPA-NXX-XXXX or NPA-511-XXXX (associated with callback information) oli parameter
Enhanced MF	Interface supports delivery of 20 digits; callback is available, location is not available	000-911-0000	NPA-NXX-XXXX or NPA-511-XXXX (associated with callback information) oli parameter
Enhanced MF	Interface supports delivery of 20 digits; location is available, callback is not available	NPA-511-XXXX (associated with location information)	000-911-0000
Enhanced MF	Interface supports delivery of 20 digits; non-initialized mobile caller, location available	NPA-511-XXXX (associated with location information)	911 + "last 7 digits of the ESN or IMEI expressed as a decimal" oli parameter
Enhanced MF	Interface supports delivery of 20 digits; neither location nor callback is available	000-911-0000	000-911-0000
Enhanced MF	Interface supports delivery of 10 digits; Callback information expected and available	NPA-NXX-XXXX or NPA-511-XXXX (associated with callback information) oli parameter	Not present
Enhanced MF	Interface supports delivery of 10 digits; Location information expected and available	NPD-511-XXXX (associated with location information) oli parameter	Not present

© Copyright 2011-2022 National Emergency Number Association, Inc.

PSAP Interface Supported	Scenario	From Header field Content	P-A-I Header field Content
Enhanced MF	Interface supports delivery of 10 digits; Callback information desired; only location information available	NPD-511-XXXX (associated with location information) oli parameter	Not present
Enhanced MF	Interface supports delivery of 10 digits; Location information desired; only callback information available	NPA-NXX-XXXX or NPA-511-XXXX (associated with callback information) oli parameter	Not present
Enhanced MF	Interface supports delivery of 10 digits; Neither callback nor location available	000-911-0000	Not present
Enhanced MF	Interface supports delivery of 10 digits; Callback information desired; call is from a non-initialized mobile	911 + "last 7 digits of the ESN or IMEI expressed as a decimal" oli parameter	Not present

6.2.2.4 SIP Re-INVITE Sent to the ESInet to Support "Silent" Emergency Calls

Upon receiving a SIP re-INVITE from the PIF component, the NIF component of the Legacy PSAP Gateway will generate a SIP re-INVITE message and send it toward the caller or Legacy Network Gateway or ingress LSRG via the ESInet. The SIP re-INVITE message will include the following information:

- A Request-URI that contains a URI from the Contact header field delivered to the Legacy PSAP Gateway or ingress LSRG in the initial INVITE message. The URI may be associated with the Legacy Network Gateway, the caller, a B2BUA, or a Conference Aware UA, as appropriate for the origination type and the transfer model implemented.
- A To header field that contains the information delivered to the Legacy PSAP Gateway in the From header field of the original INVITE message.
- A From header field that contains the digits "911" expressed as a URI (received in the To header field of the original INVITE message).

© Copyright 2011-2022 National Emergency Number Association, Inc.

- A Contact header field that contains a SIP URI associated with the Legacy PSAP Gateway along with a "urn:emergency:media-feature.tty-interworking" media feature tag.
- A Via header field that is populated with a URI associated with the Legacy PSAP Gateway.
- An SDP offer that includes a media format associated with real-time text, as described in RFC 4103 [85].

Upon receiving a 200 OK message indicating that the SDP offer associated with real-time text has been accepted, the NIF component SHALL pass the 200 OK message to the PIF component. The PIF component shall respond by sending an ACK to the NIF component, and the NIF component SHALL send an ACK toward the caller/Legacy Network Gateway/ingress LSRG.

6.2.2.5 Handling of Media Association with SMS/MMS/IM and RTT

6.2.2.5.1 Text Media Secction Establishment

As described in Section 6.2.1.4, the NIF component of the Legacy PSAP Gateway SHALL cache an incoming MSRP message and convert it to RFC 4103 real-time text for delivery to the PIF component. The NIF component MUST also facilitate the "turn-taking" expected by the TTY users involved in a conversation between an emergency caller and a legacy PSAP. Also, unless specific action is taken by the LPG, session establishment associated with SMS/IMS/IM Text to 9-1-1 messages and RTT will appear to the legacy PSAP as "silent calls". The Standard Operating Procedures associated with the processing of silent calls will result in a delay in processing the 9-1-1 call as compared to a voice 9-1-1 call. To reduce delays associated with processing silent calls, some TTY device manufacturers support a feature that causes space characters to be sent (subsequent to call establishment) as an indication that the call is from a TTY device. Some TTY users may also send space characters upon initiating a call, although this behavior cannot be relied upon. Based on the Standard Operating Procedures defined in NENA 56-004 [174], upon hearing beeping tones, the PSAP should immediately initiate a TTY/TDD call response. To improve the response time associated with SMS/MMS/IM and RTT originations, this standard recommends that the NIF component support functionality that emulates the behavior of TTY devices that generate space characters to more quickly engage TTY equipment at the legacy PSAP.

When the NIF component receives a 200 OK message from the PIF component in response to a request from the ESInet to establish an RFC 4103 text media session associated with an SMS/MMS/IM or RTT origination, it SHALL send a sequence of four (4) space characters in RFC 4103 text with 350 milliseconds of silence between each space character to the PIF

© Copyright 2011-2022 National Emergency Number Association, Inc.

component, with five (5) seconds between each sequence, until it receives an RFC 4103 text response from the PIF component.

If the NIF component does not receive a response from the PIF component (containing the interworked Baudot tones from the PSAP) within ten (10) seconds, the NIF component MUST send a preprogrammed message back to the caller that says something like "connecting to 9-1-1, please stand by". This may be repeated twice. If, after 30 seconds, no Baudot tones are received from the PSAP, the NIF component MUST send a preprogrammed message back to the caller stating, for example, that text service is not available at this time and suggesting that the user make a voice call to 9-1-1 for assistance.

6.2.2.5.2 Text Exchanges between Legacy PSAP and RTT or TTY Caller

Based on NENA 56-004, the TTY equipment at the PSAP will respond to receipt of the space character(s) by sending a preprogrammed message or an approved greeting such as "911 GA" typed by the PSAP. If the call originated as an RTT call (i.e., the media feature tag conveyed in incoming signaling associated with the emergency call has a value of "text" and no MSRP session is established with the NIF component), then upon receiving the "911 GA" in RFC 4103 text characters from the PIF component, the NIF component SHALL replace the "GA" with a line delimiter (e.g., CRLF)[77] and pass the "911" and line delimiter in RFC 4103 characters back toward the caller. If the call originated as a TTY call (i.e., the media feature tag conveyed in incoming signaling associated with the emergency call has a value of "urn:emergency:media-feature.tty-interworking"), the NIF component SHALL pass the "911 GA" received in RFC 4103 text characters from the PIF component, unchanged, back toward the caller. At this point, the text media session is established with a TTY or RTT calling user, and it is the caller's turn.

The NIF component SHALL then start an idle timer for a period of four (4) seconds as it waits for the initial text message from the caller (via the ESInet). If there is already text buffered from the caller, the NIF component SHALL send the RFC 4103 characters to the PIF component. If the NIF component receives RFC 4103 characters from the caller before the expiration of the idle timer, the NIF component SHALL convey those characters to the PIF component, initiating an inter-character timer of 4 seconds. This timer SHALL be restarted with the value 4 seconds every time a character is transmitted towards the PSAP. If the time between characters exceeds 4 seconds, the NIF component SHALL send the characters "_GA" (where the underscore indicates a space character) to the PSAP, as

[77] Insertion of a line delimiter will allow text to be presented to the SMS/MMS/IM or RTT user in a form that is more readable and expected.

© Copyright 2011-2022 National Emergency Number Association, Inc.

defined in the EAAC Report [175]. The NIF component SHALL then enter idle mode as it waits for subsequent text from the PSAP (via the PIF component) or the caller (via the ESInet). During this time the NIF component shall buffer any text received from the caller. If the NIF component detects a "_GA" from the PSAP before the expiration of the 4-second inter-character timer, the NIF component SHALL reset the inter-character timer to 1500 ms. If the NIF component receives a space, a line delimiter, or no further text before the 1500 ms timer expires, the NIF component SHALL send any buffered text characters from the caller (unchanged) to the PIF component and SHALL continue conveying text in real time from the caller. The NIF component SHALL then enter idle mode. If additional text (other than a space or line delimiter) is received from the PSAP before the 1500 ms expires, the "GA" was part of the text conversation and the the NIF component SHALL reset the 4 second timer and continue waiting for a "_GA" or line delimiter.

If the NIF component detects a line delimiter from the caller before the expiration of the 4 second inter-character timer, the NIF component SHALL replace the line delimiter with a space and SHALL reset the inter-character timer to 1500 ms. If the 1500 ms inter-character timer expires without any characters other than "_GA", or space or a line delimiter being detected, the NIF component SHALL append the characters "_GA" to the incoming RFC 4103 text and send the text characters with the "_GA" appended to the PIF component for conversion to Baudot tones. The NIF component SHALL then enter idle mode with the PSAP having the turn and any incoming text from the caller being buffered. If other characters are received from the caller within the 1500 ms timer, the NIF SHALL convey the characters to the PIF component and SHALL reset the timer to 4 seconds.

If the NIF component receives subsequent text characters from the PIF component before the expiration of the idle timer and prior to any additional text messages being received from the ESInet, it SHALL examine the text for the presence of the characters "_GA". Note that it is common for a PSAP using TTY to end a question with "Q GA". Upon detecting a " GA", the NIF SHALL set the inter-character timer to 1500 ms. If a space, line delimiter or no other characters are received within the 1500 ms time period, and the caller is a TTY caller, the characters "_GA" or "Q_GA" will be passed unchanged toward the TTY caller. The turn is then changed to be the caller's turn. If the NIF component receives a "_GA" followed by nothing other than a space or line delimiter before the 1500 ms timer expires, and the caller is an RTT caller, the NIF SHALL substitute a line delimiter for the "_GA" in the RFC 4103 text sent toward the RTT caller. In generating RFC 4103 text corresponding to the characters "Q GA" toward an RTT caller, the NIF component SHALL replace the "Q" with a "?" and SHALL replace the "GA" with a line delimiter. If other characters are received before the expiration of the 1500 ms timer, the NIF should view the "_GA" or "Q GA" as part of the contents of the conversation and SHALL pass the characters unchanged toward the caller. The NIF SHALL then continue to convey characters from the PSAP to the caller.

© Copyright 2011-2022 National Emergency Number Association, Inc.

If the NIF component detects that the call taker is sending text (i.e., it has not yet received the "_GA" from the PSAP via the PIF component), it MUST buffer any incoming text packets received from the ESInet until either the "_GA" has been received from the PSAP, or an appropriate period of time has passed without any further text being received from the PSAP. The EAAC Report [175] proposes a value of seven (7) seconds for this timer. Note that, as described above, when the NIF component buffers incoming text packets from the ESInet, it SHALL initiate a provisionable inter-character timer with a default value of 4 seconds and follow the procedures describd above. The NIF component MUST NOT send additional characters to the PIF component until it either detects a "_GA" from the PSAP or the PSAP idle timer has expired (whichever occurs first).

If the NIF component receives a "_GASK" or "_SKSK" indication from the PSAP, the NIF SHALL set the inter-character timer to 1500 ms. If a space, line delimiter or no other characters are received within the 1500 ms time period, and the caller is a TTY caller the NIF component SHALL pass these characters unchanged toward the caller. If a space, line delimiter or no other characters are received within the 1500 ms time period, and the caller is a RTT caller, the NIF component SHALL send a line delimiter toward the caller, providing handling that is consistent with what would be seen by a caller communicating with an NG9-1-1 PSAP using RTT. If other characters are received from the PSAP within the 1500 ms timer, the characters SHALL be conveyed unchanged to the caller, the NIF component SHALL reset the timer to 7 seconds and the turn will stay with the PSAP.

6.2.2.5.3 Conveyance of SMS/IMS/IM Messages to Legacy PSAPs

As described in Section 6.2.2.5.1, in support of incoming SMS/MMS/IM text to 9-1-1 messages, once an MSRP session is established with the NIF, the NIF component SHALL send a sequence of four (4) space characters in RFC 4103 text with 350 milliseconds of silence between each space character to the PIF component with five (5) seconds between each sequence until it receives an RFC 4103 text response from the PIF component. The NIF component SHALL also cache the incoming SMS/MMS/IM text to 9-1-1 message received via MSRP.

Upon determining that the call taker has joined the conversation (via receipt of an appropriate preprogrammed or typed message such as "911 GA" from the PIF component), the NIF component SHALL convert the MSRP message to RFC 4103 characters. The RFC 4103 text characters sent by the NIF component to the PIF component SHALL begin with the characters "Message" followed by the characters from the cached SMS/MMS/IM text message and the characters "_GA". The NIF component SHALL enter idle mode on its egress side and wait for the PIF/call taker to respond. The NIF component SHALL apply the same 4-second "idle timer" to MSRP conversation as it uses for RTT conversation. The NIF remains in active mode on its ingress side. When the NIF component receives RFC 4103

© Copyright 2011-2022 National Emergency Number Association, Inc.

text characters from the PIF component it SHOULD expect "_GA" or "_SKGA", possibly followed by a space or line delimiter (received within 1500 ms) at the end of the text of the message. If this is the case, the NIF component SHOULD replace the "_GA" or "_SKGA" with a line delimiter, and if there is a "Q" immediately preceding the "_GA"/"_SKGA", it should substitute a "?" for that character. If another character is received within the 1500 ms timer, the characters SHALL be conveyed unchanged toward the caller. The NIF component SHALL implement the same 7-second PSAP idle timer as described above for instances in which it does not receive "_GA" or "_SKGA". The NIF component SHALL also apply the same processing as described for RTT upon receipt of an "SKSK" or "GASK" from the PSAP.

If the NIF component detects that the caller has sent a subsequent SMS/MMS/IM message (based on receipt of an MSRP message from the ESInet), the NIF component MUST buffer the incoming MSRP message until it either receives the RFC 4103 characters "_GA" from the PIF component, or the 7-second PSAP idle timer has expired. The NIF component MUST insert the characters "_GA" at the end of the RFC 4103 text characters (converted from the MSRP message) passed to the PIF component and start buffering any subsequent incoming MSRP messages.

6.2.2.6 Support for Emergency Call Transfer

When a legacy PSAP determines that it is necessary to transfer an emergency call, it sends a "flash" signal and waits for dial tone. Once the dial tone is received, the PSAP requests the transfer either by operating a key associated with a particular type of secondary PSAP (e.g., fire department) or a particular PSAP or other transfer-to destination (e.g., using a speed calling feature), or by manually dialing the number of the desired transfer-to destination.

When the PIF component of the Legacy PSAP Gateway detects a flash, it will follow the procedures defined in RFC 4733 using code 16 for passing the "flash" signal to the NIF component of the Legacy PSAP Gateway. The PIF component will also provide dial tone to the legacy PSAP. The NIF component will interpret receipt of the flash as a request from a legacy PSAP to initiate a call transfer. In response to the dial tone, the PSAP will provide DTMF signaling in the form of a "*XX code", "# + 4 digits", or a 7/10-digit directory number. Upon receiving the "*XX" code, "# + 4 digits", or the 7/10-digit directory number of the destination party, the PIF component of the Legacy PSAP Gateway will pass the information to the NIF component using the mechanisms defined in RFC 4733. The NIF will interpret the DTMF information received from the PIF and request that a conference be created, if one has not already been created (i.e., as would be the case for networks that have implemented the Route Call Calls Via a Conference Aware UA transfer model). The NIF will then generate a SIP REFER method to request that the caller (or B2BUA,

© Copyright 2011-2022 National Emergency Number Association, Inc.

depending on the architecture being used by the ESInet to support call transfer) be invited to the conference. (Note that a REFER inviting the caller/B2BUA to the conference will only be sent by the NIF if a transfer model other than the Route All Calls Via a Conference Aware UA transfer model has been implemented.) The NIF component of the Legacy PSAP Gateway will subsequently generate another SIP REFER method to request that the conference bridge invite the transfer-to party to the conference. This latter REFER method will include an indication of the transfer-to party in the Refer-To header field. The NIF will determine the transfer-to party in one of the following ways:

- If the PIF receives a 7/10-digit destination number in the transfer request signaling from the legacy PSAP and passes this information to the NIF using the mechanisms defined in RFC 4733, the NIF SHALL use this information to populate the URI in the Refer-To header field of the outgoing REFER method.
- If the PIF receives a "# + 4-digits" in the transfer request signaling from the legacy PSAP and passes this information to the NIF using the mechanisms defined in RFC 4733, the NIF SHALL add the appropriate NPA-NXX digits at the beginning of the 4-digit string and use this information to populate the URI in the Refer-To header field of the outgoing REFER method.
- If the PIF receives a code of the form "*XX" in the transfer request signaling from the legacy PSAP and passes this information to the NIF using the mechanisms defined in RFC 4733, the NIF SHALL do one of the following, based on trunk group provisioning:
    - The NIF SHALL map the received "*XX" code to a static URI, and populate this URI in the Refer-To header field of the outgoing REFER method
    - The NIF SHALL map the received "*XX" code to a service URN and query an ECRF using this service URN and the location information received with the call.[78] The NIF will then use the URI returned in the response from the ECRF to populate the Refer-To header field of the outgoing REFER method.[79]

Figure 6-4 and Figure 6-5 provide an example of an emergency call transfer flow to illustrate different aspects of an emergency call transfer that has been requested by a legacy PSAP. Figure 6-4 shows the establishment of a conference by the Legacy PSAP Gateway in response to a transfer request from a legacy PSAP. Note that the flow

[78] Note that if the location information received with the call is a location-by-reference, the Legacy PSAP Gateway will have to first send a dereference request to a LIS or Legacy Network Gateway, using an appropriate dereferencing protocol, to obtain a routing location value for the call.

[79] This will require that the Legacy PSAP Gateway be able to map all of the *XX codes supported by each PSAP that it serves to an appropriate service URN value that it can use to obtain the associated transfer-to destination address from the ECRF.

© Copyright 2011-2022 National Emergency Number Association, Inc.

illustrated in Figure 6-4 does not apply if the Route All Calls Via a Conference Aware UA/ transfer model has been implemented. Figure 6-5 shows the completion of the transfer of the emergency call to the transfer-to PSAP. Section 3.1.1.2 provides a more complete discussion of the REFER method, and Section 4.7 provides detailed flows describing the alternatives for supporting bridging and transfer in an i3 environment.

Note: RFC 2833 defined the use of code 16 for flash. RFC 4733 obsoleted RFC 2833 but did not define a code for flash, although it did reserve code 16. Efforts will be made to restore the definition of Flash to the code registry using 16. Until such time, code 16 MUST be used as per RFC 2833.

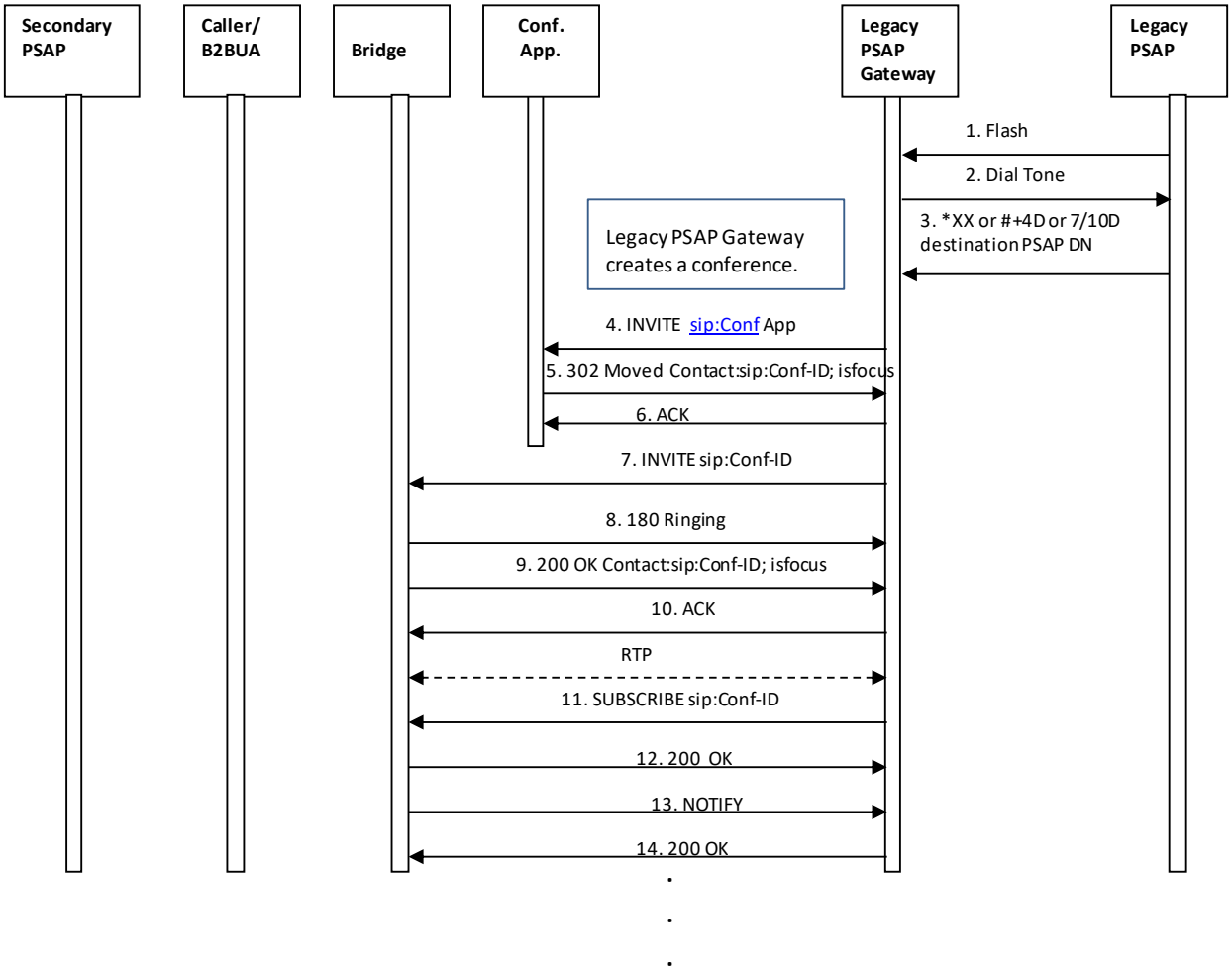


Figure 6-4 Emergency Call Transfer Request from Legacy PSAP – Conference Established

© Copyright 2011-2022 National Emergency Number Association, Inc.

The emergency call transfer flow illustrated above begins when the legacy PSAP determines that an emergency call needs to be transferred.

1. Upon determining that an emergency call needs to be transferred, the legacy PSAP initiates a transfer request by sending a flash signal to the Legacy PSAP Gateway.
2. When the Legacy PSAP Gateway receives the flash signal, it returns dial tone to the legacy PSAP and prepares to receive DTMF signaling.
3. The legacy PSAP provides a "*XX code", a string consisting of "# + 4-digits", or the 7/10-digit directory number associated with the transfer-to PSAP/public safety agency.
4. The Legacy PSAP Gateway creates a conference by first sending an INVITE to a conference application, using a URI that is known or provisioned at the Legacy PSAP Gateway.
5. The Conference Application responds by sending a 302 Moved message that redirects the Legacy PSAP Gateway to the conference bridge and provides the Conference-ID that should be used for the conference.
6. The Legacy PSAP Gateway acknowledges the receipt of the 302 Moved message.
7. The Legacy PSAP Gateway generates an INVITE to establish a session with the conference bridge.
8. The conference bridge responds to the INVITE by returning a 180 Ringing message.
9. The conference bridge then returns a 200 OK message, and a media session is established between the Legacy PSAP Gateway and the conference bridge.
10. The Legacy PSAP Gateway returns an ACK message in response to the 200 OK.
11. through 14. Once the media session is established, the Legacy PSAP Gateway subscribes to the conference URI obtained from the Contact URI provided in the 200 OK message from the conference bridge.

After the Legacy PSAP Gateway establishes the conference, it sends a REFER method to the conference bridge asking it to invite the caller/B2BUA to the conference, following the procedures described in Sections 4.7.1.1 and 4.7.1.2. (Note that a REFER requesting that the bridge invite the caller/B2BUA to the conference will not be sent if the Route all Calls Via a Conference Aware UA transfer model is implemented.) Once the conference bridge has done so, the Legacy PSAP Gateway asks the conference bridge to invite the transfer-to party to the conference. It does this by generating a REFER method with a Refer-To header field that contains the URI of the transfer-to PSAP/agency, determined using one of the methods described above. The REFER SHOULD include any location information associated with the original caller that was received in the initial INVITE message in an escaped Emergency Incident Data Object (EIDO), as described below. The EIDO SHALL also include callback information. The Legacy PSAP Gateway will populate the remaining fields of the REFER based on RFC 3515.

© Copyright 2011-2022 National Emergency Number Association, Inc.

As described in Section 4.7, the Legacy PSAP Gateway SHALL be capable of receiving a 200 OK message in response to the REFER, followed by a NOTIFY that contains the status of the REFER request. The Legacy PSAP Gateway then returns a 200 OK in response to the NOTIFY.

When the call to the transfer-to PSAP is answered, the Legacy PSAP Gateway will receive a NOTIFY message indicating this event. The Legacy PSAP Gateway SHALL respond to the NOTIFY by returning a 200 OK message.

The Legacy PSAP Gateway SHALL create an EIDO, as described in the EIDO JSON standard [111] that contains location information (by value or reference), as well as any Additional Data blocks received by the Legacy PSAP Gateway with the call. The EIDO SHALL also contain callback information. The Legacy PSAP Gateway SHALL pass this information to the transfer-to PSAP via the conference bridge. If the Additional Data was received by value, it SHALL be sent in the EIDO by value, and if it was received by reference, it SHALL be sent in the EIDO by reference. While the Legacy PSAP Gateway does not know all of the information the transfer-from PSAP developed in its handling of the call, it SHOULD pass what it does know to the transfer-to PSAP using this mechanism.

When the transfer-from PSAP determines that it should drop off the conference and complete the transfer, it SHALL follow the steps illustrated below.

© Copyright 2011-2022 National Emergency Number Association, Inc.

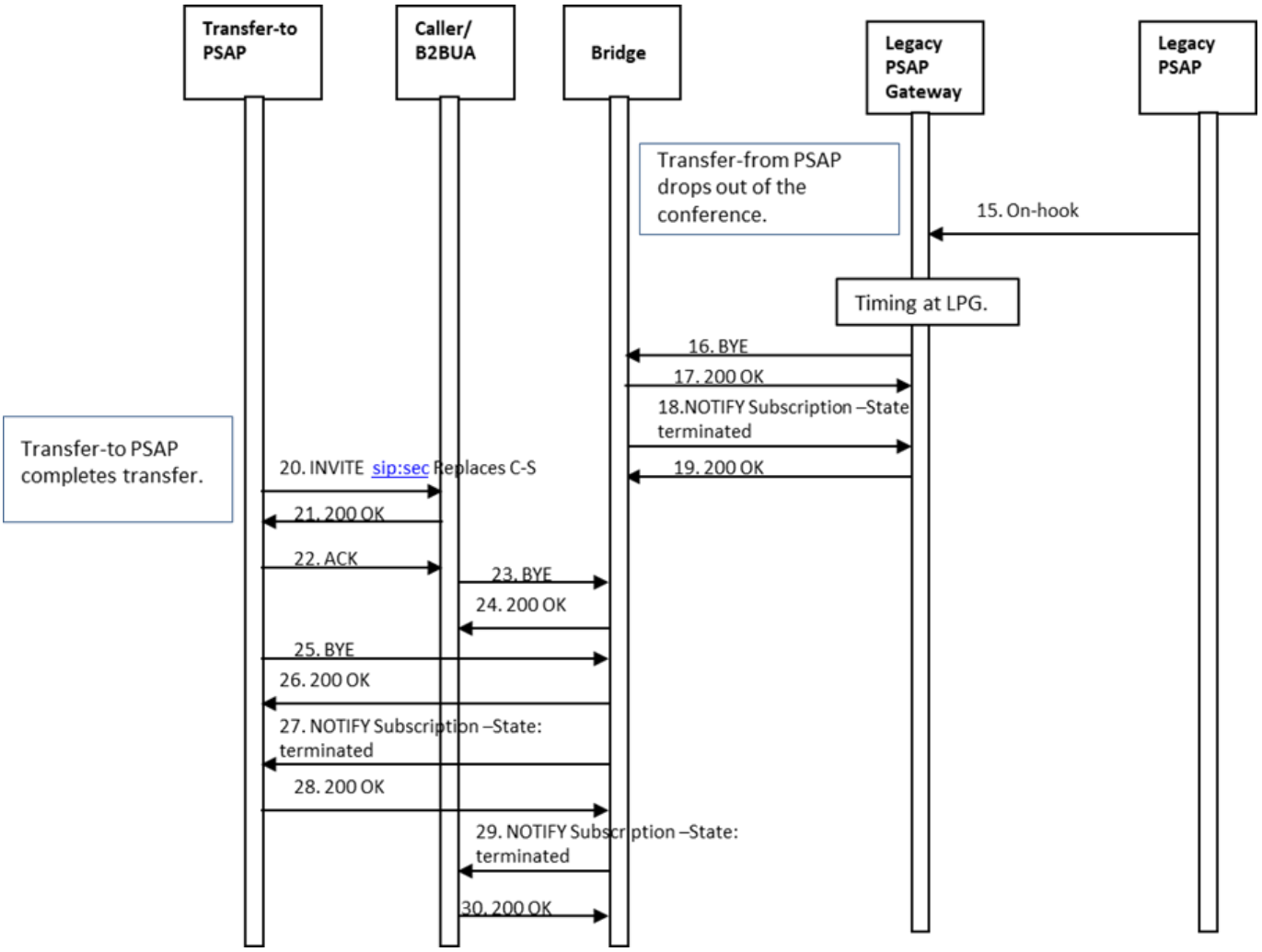


Figure 6-5 Emergency Call Transfer Request from Legacy PSAP – Transfer Completed

The emergency call transfer flow illustrated above begins when the legacy PSAP determines that it can drop off the conference with the caller and the transfer-to PSAP and complete the transfer.

15. Upon determining that the emergency call transfer should be completed, the legacy PSAP disconnects from the call by sending an on-hook signal to the Legacy PSAP Gateway.

The Legacy PSAP Gateway sets a timer for 1.1 seconds to distinguish a disconnect indication from a flash signal.

© Copyright 2011-2022 National Emergency Number Association, Inc.

16. When the Legacy PSAP Gateway determines that the PSAP has disconnected, it sends a BYE message to the conference bridge.
17. The conference bridge responds by returning a 200 OK message.
18. The conference bridge then returns a NOTIFY message indicating that the subscription to the conference has been terminated.
19. The Legacy PSAP Gateway returns a 200 OK in response to the NOTIFY.
20. If applicable, based on the transfer model used, the transfer-to PSAP completes the transfer by sending an INVITE to the caller/B2BUA requesting that they replace their connection to the bridge with a direct connection to the transfer-to PSAP.
21. The caller/B2BUA responds by returning a 200 OK message.
22. The transfer-to PSAP responds by returning an ACK to the caller/B2BUA.
23. The caller/B2BUA then sends a BYE to the conference bridge to terminate the session.
24. The conference bridge responds by sending the caller/B2BUA a 200 OK message.
25. The transfer-to PSAP also terminates its session with the conference bridge by sending a BYE message.
26. The conference bridge responds by sending a 200 OK message to the transfer-to PSAP.
27. The conference bridge then returns a NOTIFY message to the transfer-to PSAP indicating that the subscription to the conference has been terminated.
28. The transfer-to PSAP responds with a 200 OK message.
29. The conference bridge sends a NOTIFY message to the caller/B2BUA indicating that the subscription to the conference has been terminated.
30. The caller/B2BUA responds with a 200 OK message.

The LPG MUST handle the case of a transfer between two legacy PSAPs that it serves.

6.2.2.7 Alternate Routing Invocation and Notification

Alternate routing allows a network to temporarily re-route calls to a different PSAP when the primary PSAP is unavailable to answer the call, or when connectivity to the primary PSAP is not available due to network failure.

In a legacy environment, when a PSAP determines that alternate routing needs to be manually invoked (e.g., the PSAP needs to evacuate), it calls the alternate PSAP to inform them of the situation, so they are prepared to begin to receive all of the primary PSAP's calls. Today, the capability to manually invoke/cancel alternate routing is controlled by the primary PSAP. Typically, when alternate routing is to be invoked, the primary PSAP manually activates a switch or other control item to change the state of a control circuit connected to a scan point or other sensing device at the SR. When the state of the circuit is changed (e.g., by "shorting out" the circuit or closing a relay on a Network Control

© Copyright 2011-2022 National Emergency Number Association, Inc.

Module [NCM]), the scan points get saturated and, from the perspective of the SR, it appears as an "all circuits busy" condition on the trunk group. This causes the SR to route calls intended for the primary PSAP to the alternate PSAP. To remove alternate routing, the primary PSAP restores the normal state of the control circuit (or re-opens the relay(s) at the NCM). In some cases, manual alternate routing is invoked when the primary PSAP places a call to their E9-1-1 System Service Provider to request that action. This is also something a Legacy PSAP Gateway MUST be able to replicate.

In an i3 Solution environment, a Legacy PSAP Gateway MUST be capable of recognizing a request to activate alternate routing. This request may come in the form of a physical switch, or it may be made via a GUI or web server. Upon detecting the alternate routing request, the Legacy PSAP Gateway MUST generate a ServiceState change event notification back to the ESRP to inform it of the change in PSAP state. Note that, using this event notification mechanism, the ESRP will be able to distinguish between alternate routing that is due to traffic volumes (i.e., events related to queue state) and "make busy" scenarios, in which the PSAP is experiencing some type of failure or evacuation situation (i.e., events related to PSAP state). It is assumed that the policy rules associated with alternate routing requests related to a specific PSAP will have been previously populated in the PRF.

6.2.2.8 Test Calls

The NIF MUST support and act as the termination point for the test call interface although administrative provisioning processes SHOULD be available to disable it, especially under overload situations. The test interface includes the ability of the test caller to offer media and to receive a response and loop back a small number of packets of each media accepted at the PSAP. This provides a mechanism for a caller to determine that a call to a legacy PSAP behind a Legacy PSAP Gateway could not accept video. Legacy PSAP Gateways MUST refuse offers for video and accept offers for audio and text (which will be converted by the PIF component and conveyed using existing mechanisms, i.e., TTY). The LPG is responsible for the media loopback required by the test call mechanism. Test calls SHOULD NOT be passed through the LPG to the Legacy PSAP.

6.2.2.9 Handling of Advanced Automatic Crash Notification Calls

As described in Section 3.1.19, when an NG-AACN call is presented to the ESInet, the SIP INVITE message associated with that call will contain a VEDS telematics dataset and a metadata/control object indicating the capabilities of the vehicle/TSP. If the NIF component of the Legacy PSAP Gateway receives such a SIP INVITE message, it SHALL NOT attach a metadata/control object to its final response to the SIP INVITE message. This will convey to the vehicle or TSP that the call is not end-to-end NG-AACN and will cause the

© Copyright 2011-2022 National Emergency Number Association, Inc.

vehicle/TSP to fall back to legacy mechanisms for conveying crash and location data (e.g., using text-to-speech, pre-recorded audio, or verbal interaction with the TSP assistant).

6.2.3 Location Interwork Function (LIF)

As described in Section 6.2, the Legacy PSAP Gateway MUST support an ALI interface that can accept an ALI query from the legacy PSAP and return location information based on the formats specified in NENA-STA-027 [164] and NENA 04-005 [165]. There is additional information beyond just callback number and location information that may be included in an ALI response. There are various ways that ALI data may be obtained by the Legacy PSAP Gateway so that it can be returned to the legacy PSAP in the expected format.

If the Legacy PSAP Gateway receives callback information (i.e., in the form of a 10-digit NANP number) and location-by-value in the incoming INVITE message from the ESRP, the Legacy PSAP Gateway can use this information to populate the callback number and location fields of the ALI response. Note that the Legacy PSAP Gateway will have to interact with the MSAG Conversion Service (MCS) if the location information received in incoming signaling (or obtained via dereferencing) is in civic format. This is necessary to ensure that the location information populated in the ALI response message is in the correct format for the legacy PSAP to which it is being delivered. (See Section 4.4 for further details regarding the MCS.) If the interaction with the MCS is unsuccessful, the Legacy PSAP Gateway will provide an indication of "no record found" to the PSAP.

If the legacy PSAP Gateway receives callback information in the incoming INVITE message from the ESRP that is not in the form of (or easily converted to) a 10-digit NANP number, the Legacy PSAP Gateway SHALL populate the pANI generated by the NIF component (as described in Section 6.2.2.1) as the callback number in the ALI response.

If location-by-reference is received in the incoming INVITE message from the ESRP, the Legacy PSAP Gateway SHALL support the ability to query other elements (i.e., LISes, Legacy Network Gateways) using an appropriate dereferencing protocol, as specified in Section 3.2, to obtain caller location for the call. If the location value returned in the dereference response is a civic location, the Legacy PSAP Gateway will use the MCS and convert the caller location value to the appropriate format for population in the ALI response message.

If the location-by-value received in a SIP INVITE message from an ESRP or in a dereference response contains a geodetic coordinate-based location that identifies a shape other than a point or circle with radius, the Legacy PSAP Gateway MUST convert that geo-coordinate location to a point with uncertainty, using an appropriate algorithm, before populating it in the ALI response message.

© Copyright 2011-2022 National Emergency Number Association, Inc.

The Legacy PSAP Gateway will use Additional Data structures to populate other fields in the ALI response. If the Additional Data has been delivered to the Legacy PSAP Gateway "by-reference", the Legacy PSAP Gateway SHALL support the HTTPS GET method described in IETF RFC 7230 [162] to obtain the Additional Data "by-value"[80]. The Legacy PSAP Gateway SHALL use the information contained in the Call-Info header field of the received INVITE to either identify the address of the target ADR to which the GET will be directed, or the place in the message body where the Additional Data is provided "by-value". The Legacy PSAP Gateway SHALL be capable of processing the XML-formatted Additional Data structures in the message body or received in the dereference response and using it to populate the appropriate fields of the ALI response message. The Additional Data used to populate the ALI response comes from the data in the call signaling and not from the data in the PIDF-LO.

See Appendix A for a detailed description of where the Legacy PSAP Gateway will obtain the necessary information to populate ALI response messages.

6.2.4 Timing at the Legacy PSAP Gateway

6.2.4.1 Call Setup Timing

Call Setup timing SHALL be used by the PIF component of the Legacy PSAP Gateway to determine if the legacy PSAP CPE is correctly interfacing with the Legacy PSAP Gateway. Call Setup timing for Enhanced MF (E-MF) and Traditional MF (NPD + 7-digit ANI) is the same, so only one example of setup timing will be outlined. Precise details of Call Setup timing can be found in NENA 03-002 [163], ATIS-0900414.2012(R2017) [192], and/or Telcordia GR-350--CORE [189].

Legacy 9-1-1 system policies dictate that a 9-1-1 call is terminated if it encounters two successive call setup failures. If the Legacy PSAP Gateway cannot deliver a call to a legacy PSAP trunk on the first attempt, it SHALL then attempt to deliver the call to another PSAP trunk, according to its standard hunting or routing algorithms. If the Legacy PSAP Gateway has a call setup failure on the second attempt, it SHALL terminate the call, and return an appropriate message (i.e., a SIP 500 Server Internal Error message) toward the originating network(s) to indicate such.

---

[80] Legacy PSAPs do not differentiate between access networks and originating networks. Additional Data from the access network may be present in a PIDF-LO received by the LPG as well as Additional Data from the originating network received via a Call-Info header field. The LPG uses the originating network information in the Call-Info header field instead of any access network Additional Data in the PIDF-LO. Devices and Service providers other than the access and originating networks may provide Additional Data. The LPG does not send this data to the PSAP.

© Copyright 2011-2022 National Emergency Number Association, Inc.

The Legacy PSAP Gateway SHALL determine that a call setup has or will fail when the PIF component fails to receive a wink from the CPE in response to its off-hook condition (Seizure) toward the legacy PSAP within a specific period of time. Traditional values would suggest that the PSAP return a wink to the Legacy PSAP Gateway within a minimum of four (4) to twenty (20) seconds. Most 9-1-1 systems use the four-second interval as the minimum time period in order to reduce potential call delays on a first try failure. If the Legacy PSAP Gateway has not received a wink condition from the PSAP CPE within the minimum period (i.e., four seconds) after sending an off-hook indication, it SHALL mark the call as a failure, and proceed as described above (i.e., by sending a SIP 500 Server Internal Error message toward the originating network).

6.2.4.2 Call Disconnect Timing

Call disconnect timing depends on whether the caller[81] or the PSAP disconnects first. It determines how soon the Legacy PSAP Gateway may offer a new call to the legacy PSAP on the same circuit. The Legacy PSAP Gateway MUST ensure that there is sufficient timing between the disconnection of one call and the presentation of a new call to the legacy PSAP so that the legacy PSAP CPE can reset and be ready in time for the next call.

6.2.4.2.1 Call Disconnect Timing When PSAP Disconnects First

If the PSAP disconnects first, the Legacy PSAP Gateway SHALL wait a sufficient time period after the receipt of the on-hook signal from the CPE to determine that the on-hook condition is a disconnect, and not a hook flash (i.e., a request to generate or cancel a three-way conference). In most legacy implementations, the minimum time period is generally assumed to be approximately 1100 ms to consider the on-hook condition a disconnect request. At this point, the Legacy PSAP Gateway may offer a new call to the Legacy PSAP.

6.2.4.2.2 Call Disconnect Timing When Caller Disconnects First

If the caller disconnects (resulting in the Legacy PSAP Gateway sending an on-hook signal to the legacy PSAP) prior to the legacy PSAP disconnecting, the Legacy PSAP Gateway MUST wait a sufficient period of time after the PSAP has gone into an on-hook condition so that it is ready to respond to a new call being offered from the Legacy PSAP Gateway. This is sometimes described as a guard interval. Industry has not yet established a typical value for this timer. It varies by system, and by PSAP CPE type. Typical minimum values are: 700

[81] Note that in some jurisdictions, certain wireline-type services support PSAP Call Control features disallowing the caller to disconnect first. See Appendix C- Support for PSAP Call Control Features (Normative) for details.

© Copyright 2011-2022 National Emergency Number Association, Inc.

ms, 1250 ms, or even 1650 ms between the on-hook condition from the PSAP CPE and the Legacy PSAP Gateway offering a new call to the legacy PSAP. (Under no circumstances SHALL the Legacy PSAP Gateway offer a call to the legacy PSAP when the legacy PSAP is still in an off-hook condition toward the Legacy PSAP Gateway.) The Legacy PSAP Gateway may set this guard timer value as appropriate for the CPE type, but MUST NOT offer new calls until a minimum interval after an on-hook indication has been received by the Legacy PSAP Gateway from the legacy PSAP CPE.

6.2.5 Trouble Detection/Reporting at the Legacy PSAP Gateway

The Legacy PSAP Gateway SHALL generate messages, alarms, etc. when it encounters problems with a legacy PSAP. The conditions under which a Legacy PSAP Gateway SHALL generate such messages/alarms shall include:

- PSAP initiates a request for alternate routing/activates a make-busy switch
- The Legacy PSAP Gateway detects a wink failure
- A PSAP trunk stays in an off-hook condition longer than expected (keeping a circuit from being used).

It is also desirable that the Legacy PSAP Gateway allows one or more members or circuits to a legacy PSAP to be taken out of service as necessary to test, modify, or manage the network.

7 Data and the Emergency Incident Data Object

With the implementation of NG9-1-1 there will be many forms of additional data available to policy routing rules, PSAPs and responders. Additional Data is communicated by reference or by value in the SIP INVITE and MESSAGE, in the PIDF-LO, or within responses to queries against IS-ADR functional elements or ADR URIs obtained from an ECRF. Additional Data has many conceivable uses, including informing telecommunicators and first responders, and providing a means to drive call routing and handling rules which look beyond caller location alone. Data generated by the PSAP while handling the call is captured in an Emergency Incident Data Object (EIDO) and passed to other agencies that are involved with the incident.

Note: Specification for the conveyance of EIDOs between agencies, systems, and applications will appear in a future version of this document.

7.1 Additional Data

Any of the additional data elements in RFC 7852 [107], NG9-1-1 Additional Data, National Emergency Number Association, NENA 71-001 [73], or its successor document,

© Copyright 2011-2022 National Emergency Number Association, Inc.

NENA-STA-012.2.-2017 [193] may be used by PSAP management to establish business rules/policies for call handling and routing.

Additional Data is defined as a set of blocks, with each block having different kinds of data contained within it. One block type is used to identify the provider of the data. Each block is passed individually. Additional Data is conveyed by reference or by value via a Call-Info header fields, or via URIs obtained from an ECRF, or by searching an IS-ADR. Dereferencing the URI is accomplished with an HTTPS GET (with fallback to HTTP if appropriate). ESInet elements use credentials traceable to the PCA, which must be accepted by the entity holding the data. Any source can provide any of the blocks registered in the IANA Emergency Call Data registry [179], but the following table provides examples of typical sources of blocks of Additional Data:

Table 7-1 Typical Sources of Additional Data

Block	Typical Source
ProviderInfo	All
ServiceInfo	Originating Network or Service Provider
DeviceInfo	Device, Originating Network, or Service Provider
SubscriberInfo	Device, Originating Network, or Service Provider
Comment	All
VEDS	Vehicle or Telematics Service Provider

The sources listed are not exclusive. In the above table, the device, originating network or caller could operate an ADR containing the data itself, or it could supply the data to a 3rd party which operates the ADR, or it can include the data by value in the call. Any intermediary (service provider) handling the call MUST provide a ProviderInfo block. Per RFC 7852 [107], when no originating network or service provider is in the path of the call, the calling device MUST provide Additional Call Data.

Section 3.1.15 Originating Network Interface requires every emergency call to include certain Additional Data blocks conveyed via Call-Info header fields with an "EmergencyCallData" prefixed purpose parameter. Calls may include further Call-Info header fields with an "EmergencyCallData" prefixed purpose. The device MAY insert one for its DeviceInfo block and one for its ProviderInfo block, and an intermediary MAY insert its own set. When there are multiple intermediaries, each intermediary MAY insert a set for the blocks it is supplying. For example, a telematics service provider may provide one and the mobile carrier handling the call may provide one. (See Section 3.1.19 for more information about telematics calls and datasets.)

© Copyright 2011-2022 National Emergency Number Association, Inc.

To protect the privacy of the caller, the amount of information returned by the ADR query may vary depending on the TLS session credentials established by the entity executing the query. PSAPs SHALL have credentials traceable to the PCA that MUST be accepted by the data provider.

Ultimately, a given call may have multiple sources of Additional Data from one or more ADRs. If conflicting information is discovered, the information identified as most recently updated by the data source SHALL take precedence over information determined to be older. See the note at the end of Section 4.2.2.5 Additional Data Interfaces.

Additional Data received by reference MUST be passed by reference to any other entities. Additional Data URIs obtained from an ECRF may be added to the call in Call-Info header fields, as discussed in Section 4.2.2.5 Additional Data Interfaces.

7.2 Additional Data associated with a PSAP, the Emergency Incident Data Object

The Emergency Incident Data Object (EIDO) is defined in the NG9-1-1 Emergency Incident Data Object (EIDO) [111].

When a PSAP handles a call, it develops information about the call which MAY be passed to subsequent PSAPs' dispatchers and/or responders. A reference to this structure SHALL be passed with a transferred call (see Section 4.7.4) and, if the transferred-to party wishes to obtain the EIDO as part of a dispatch operation, the structure MUST be retrieved using the EIDO Conveyance mechanisms defined in NENA/APCO-STA-024.1-201x [185] (work in progress).

8 3rd Party Origination

Service providers who operate call centers and wish to facilitate emergency calls from their subscribers with the call center agent remaining on the line (i.e., initially a three-way call with the caller, the call agent and the PSAP call taker) MAY use 3rd Party Origination.

The caller is assumed to have a two-way SIP call between the caller and the call agent. Service providers who do not use SIP between the caller and the call agent MAY use a gateway to interwork the call signaling from the caller to SIP and MUST similarly use a gateway to interwork the signaling from the call agent to the caller from SIP. In such cases, the following signaling description applies, even though the call starts without a SIP call between the caller and call agent.

8.1 3rd Party Client is Referred to PSAP; PSAP Establishes Conference

In the first portion of the flow, the 3rd party client has encountered an emergency situation and a call is placed to the 3rd party call agent. The 3rd party call agent requests that the

© Copyright 2011-2022 National Emergency Number Association, Inc.

caller initiate an emergency call. Upon receiving an emergency session request that contains an indication of referral by a 3rd party agency, the PSAP establishes a session with a conference bridge and requests that the bridge refer the 3rd party call agent to the conference.

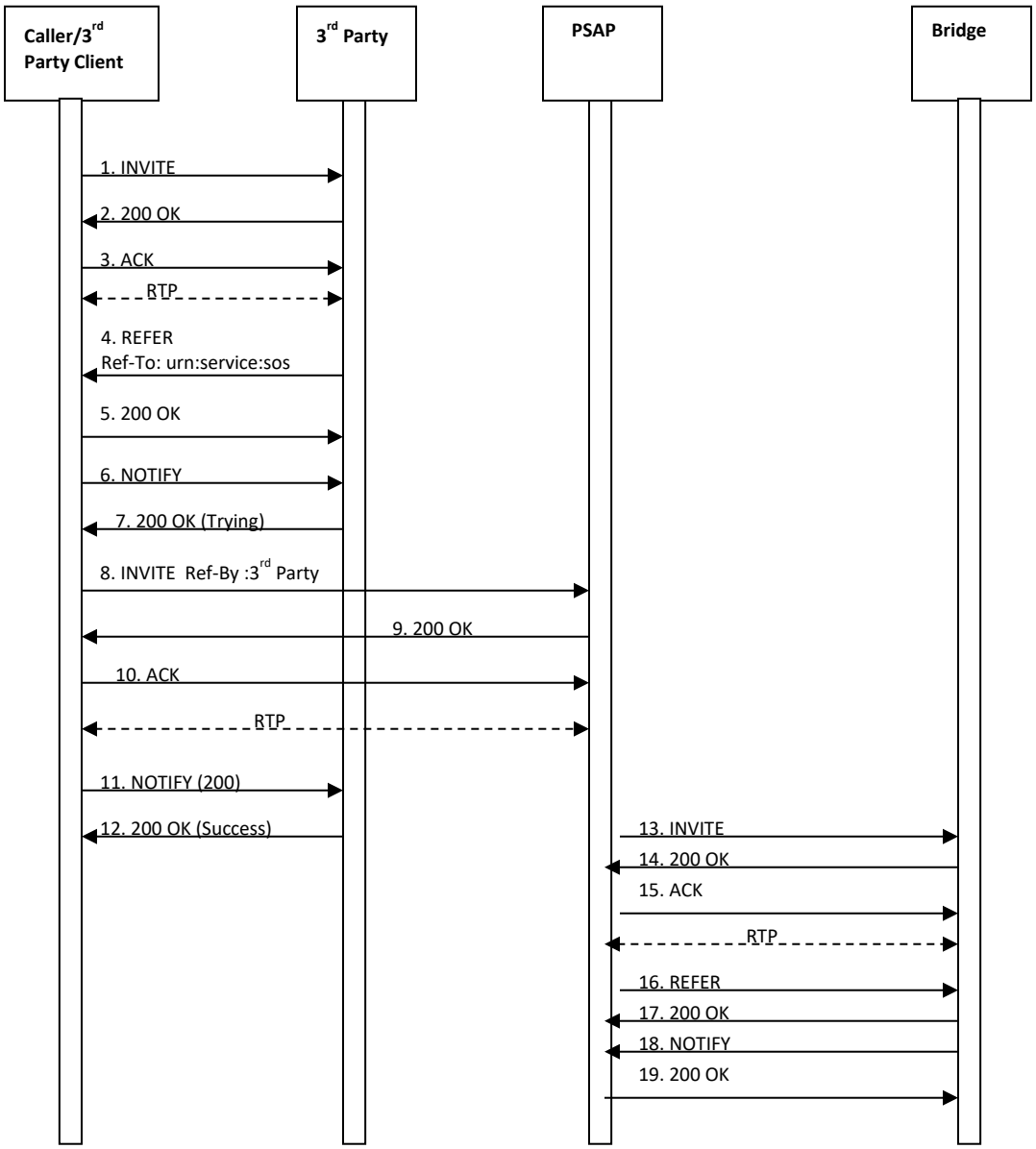


Figure 8-1 3rd Party Origination Call Flow – PSAP Conference

1. Upon encountering an emergency situation, an INVITE message is sent by a 3rd party client requesting that a session be established with a 3rd party call agent.

© Copyright 2011-2022 National Emergency Number Association, Inc.

2. The 3rd party call agent responds to the INVITE message by returning a 200 OK message.
3. The caller/3rd party client returns an ACK to the 3rd party call agent in response.

At this point a session is established between the caller/3rd party client and the 3rd party call agent. The agent determines that a 9-1-1 call is required.

4. The 3rd party call agent sends a REFER message to the caller/3rd party client with a Refer-To header field containing the destination "urn:service:sos", which indicates that an emergency session request should be initiated. Note that the call agent includes an Additional Data URI in an escaped Call-Info header field in the REFER.
5. The caller/3rd party client responds by returning a 200 OK message to the 3rd party call agent.
6. The caller/3rd party client also returns a NOTIFY message, indicating the subscription state of the REFER request (i.e., active).
7. The 3rd party call agent returns a 200 OK message in response to the NOTIFY message.
8. The caller/3rd party client then initiates an emergency call by sending an INVITE message to "urn:service:sos". This INVITE is a normal 9-1-1 call, and has all of the content specified by RFC 6881 [46]. This INVITE message contains a Referred-by header field [28]indicating that this emergency session request is associated with a REFER that was generated by a 3rd party call agent. It also includes the Additional Data URI that it received in the escaped Call-Info header field in the REFER from the 3rd party call agent.
9. When the PSAP receives the emergency session request with the Referred-By header field, it returns a 200 OK message to the caller/3rd party client.
10. The caller/3rd party client responds by returning an ACK to the PSAP.

At this point, a session is established between the caller/3rd party client and the PSAP.

11. The caller/3rd party client sends a NOTIFY message to the 3rd party call agent updating the status of the REFER request.
12. The 3rd party call agent responds by returning a 200 OK confirming the success of the REFER.
13. Based on receipt of the Referred-By header field in the INVITE message from the caller/3rd party client indicating a need for a bridge to handle a 3-way call, the PSAP sends an INVITE to its conference bridge to establish a session with the bridge.
14. The bridge responds by returning a 200 OK message to the PSAP.
15. The PSAP responds by sending an ACK to the bridge.
16. The PSAP sends a REFER message to the bridge requesting that it invite the 3rd party call agent to the conference.
17. The bridge responds by sending a 200 OK message to the PSAP.

© Copyright 2011-2022 National Emergency Number Association, Inc.

18. The bridge then sends a NOTIFY message indicating the status of the REFER request.
19. The PSAP responds to the NOTIFY by returning a 200 OK message to the bridge.

8.2 3rd Party Call Agent and Caller Added to Conference

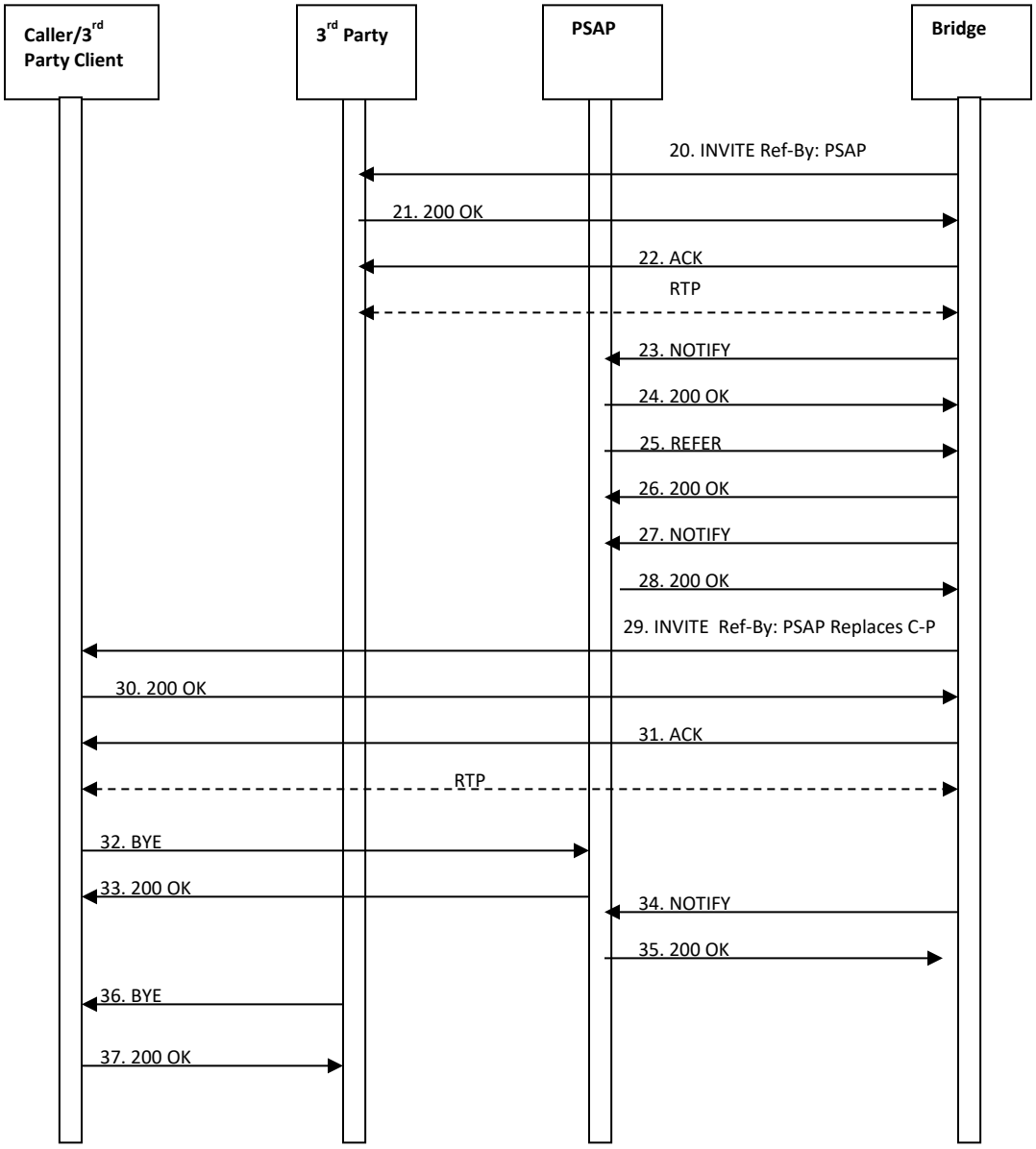


Figure 8-2 3rd Party Call Agent - Caller Added

© Copyright 2011-2022 National Emergency Number Association, Inc.

20. The bridge sends an INVITE message to the 3rd party call agent. The INVITE contains an indication in a Referred-by header field [28] that it is related to a REFER initiated by the PSAP.
21. The 3rd party call agent responds by returning a 200 OK message to the bridge.
22. The bridge returns an ACK to the 3rd party call agent.

At this point a session is established between the 3rd party call agent and the bridge.

23. The bridge sends a NOTIFY message to the PSAP indicating the status of the REFER request.
24. The PSAP responds by returning a 200 OK message.
25. The PSAP then sends a REFER message to the bridge requesting that it invite the caller/3rd party client to the conference. The REFER includes a Replaces header field to indicate to the caller/3rd party that the session with the bridge replaces its existing session with the PSAP.
26. The bridge responds by sending a 200 OK message to the PSAP.
27. The bridge then sends a NOTIFY message to the PSAP indicating the status of the REFER request.
28. The PSAP responds by returning a 200 OK message.
29. The bridge then sends an INVITE message to the caller/3rd party client asking that they replace their connection to the PSAP with a connection to the bridge.
30. The caller/3rd party client responds by returning a 200 OK message to the bridge.
31. The bridge responds by returning an ACK to the caller/3rd party client.

At this point the caller/3rd party client has established a session with the bridge.

32. The caller/3rd party client then sends a BYE message to the PSAP to terminate its session with the PSAP.
33. The PSAP responds by sending a 200 OK message to the caller/3rd party client.
34. The bridge sends a NOTIFY message to the PSAP indicating the status of the REFER request.
35. The PSAP responds by sending a 200 OK message to the bridge.
36. The 3rd party call agent sends a BYE message to the caller/3rd party client to terminate the session it had with the caller/3rd party client.
37. The caller/3rd party client responds by returning a 200 OK to the 3rd party call agent.

The above sequence assumes that the caller/3rd party client has the most accurate location information to route and dispatch the call. In some circumstances, the 3rd party call agent may have better location. It can supply the location in an EIDO, or it can arrange to have the caller/3rd party client send its emergency call INVITE (Step 8) through the 3rd party call agent and add the more accurate location to the call.

© Copyright 2011-2022 National Emergency Number Association, Inc.

Either the 3rd party client or the caller can initiate the disconnection of the original session between them (Step 36).

9 Test Calls

NG9-1-1 PSAPs MUST implement the test function described in RFC 6881 [46]. As the function is designed to test if a 9-1-1 call was placed from the test-initiating device, the test mechanism SHOULD mimic the entire actual 9-1-1 call path as closely as practical. The test mechanism is completely automatic, with no manual intervention required. To route the same as an actual emergency call, route urns in the "urn:emergency:service" tree are provided for test calls.

An INVITE message with the Service URN (found in the Request-URI) of "urn:service:test.sos" SHALL be interpreted as a request to initiate a test call. The PSAP SHOULD return a 200 OK response in normal conditions, indicating that it will complete the test function. The PSAP MAY limit the number of test calls. If that limit is exceeded, the response MUST be 486 Busy Here. PSAPs MAY accept requests for sub-services such as "urn:service:test.sos.fire." and complete a test call, or the PSAP MAY reject the call and return 404 Not Found. PSAP management MAY disable the test function (using PSAP policy).

If the PSAP accepts the test, it SHOULD return in the 200 OK a body with MIME type text/plain consisting of the following contents:

a. The name of the PSAP, terminated by a CR and LF;
b. The string "urn:service:test.sos" terminated by a CR and LF;
c. The location reported with the call (in the Geolocation header field). If the location was provided by value, the response would be a natural text version of the received location. If the location was provided by reference, the PSAP SHOULD dereference the location, using credentials acceptable to the LIS issued specifically for test purposes. Credentials issued by a PCA-rooted CA MUST have the token "test" as the agent name or the first token in the FQDN. The location returned may not be the same as the LIS would issue for an actual emergency call.

The PSAP SHOULD insert its identity in the Contact header field of the response. To provide authentication, the Identity header field (RFC 8224 [60]) SHOULD be inserted, signed by an entity in the path (such as an ESRP) with a certificate traceable to the PCA.

A PSAP accepting a test call SHOULD accept a media loopback test (RFC 6849) [100] and SHOULD support the "rtp-pkt-loopback" and "rtp-start-loopback" options. The PSAP user agent would specify a loopback attribute of "loopback-source", the PSAP being the mirror. The PSAP SHOULD loop back no more than 3 packets of each media type accepted (voice, video, text), after which the PSAP SHOULD send BYE.

© Copyright 2011-2022 National Emergency Number Association, Inc.

PSAP CPE SHOULD refuse repeated requests for test from the same device (same Contact URI or source IP address/port) in a short period of time (within 2 minutes). Any refusal is signaled with a 486 Busy Here.

Note: A PSAP Management interface will be provided in a future version of this document.

10 IANA Actions

Registries mentioned below are all within the "emergency" registry.

10.1 "urn:emergency" namespace

IANA is requested to add the following values to the urn:emergency registry.

Name	Purpose	Reference
service	Internal LoST queries	This document
policy	Route Policy	This document
normalnexthop	Normal route for Route Policy	This document
servicenotimplemented	Error response for no service within boundary of ECRF	This document
media-feature	TTY interworking and PSAP Call Control features	This document
uid	Unique identifiers	This document

10.2 "urn:emergency:service" URN Subregistry

IANA is requested to add the following values to the urn:emergency:service registry

Name	Purpose	Reference
additionalData	Return a URI to an Additional Data block	This document
serviceAgencyLocator	Return a URI to a Service or Agency	This document
psap	Return a URI to a PSAP	This document
responder	Routing emergency calls within the ESInet towards a responder.	This document
sos	Routing emergency calls within the ESInet toward a primary PSAP call taker.	This document

10.3 "urn:emergency:service:sos" Registry

IANA is requested to add the following values to the urn:emergency:service:sos registry

© Copyright 2011-2022 National Emergency Number Association, Inc.

Name	Purpose	Reference
psap	Route calls to primary PSAP.	This document
call_taker	Route calls to a call taker within a PSAP.	This document
level_2_esrp	Route calls to a second level ESRP (for an example, a state ESRP routing towards a county ESRP)	This document
level_3_esrp	Route calls to a third level ESRP (for example, a regional ESRP that received a call from a state ESRP and in turn routes towards a county ESRP).	This document

10.4 "urn:emergency:service:test" Registry

IANA is requested to add the following values to the urn:emergency:service:test registry

Name	Purpose	Reference
psap	Route test calls to primary PSAP	This document
call_taker	Normally not used, but some implementations may make use of this urn	This document
level_2_esrp	Route test calls to a second level ESRP (for an example, a state ESRP routing towards a county ESRP)	This document
level_3_esrp	Route test calls to a third level ESRP (for example, a regional ESRP that received a call from a state ESRP and in turn routes towards a county ESRP).	This document

10.5 "urn:emergency:service:responder" Registry

IANA is requested to add the following values to the urn:emergency:service:responder registry

Name	Description	Reference
coast_guard	Coast Guard station	This document
ems	Emergency Medical Service	This document
fire	Fire Department	This document
mountain_rescue	Mountain Rescue Service	This document
poison_control	Poison Control Center	This document
police	Police Agency	This document

© Copyright 2011-2022 National Emergency Number Association, Inc.

Name	Description	Reference
psap	other purposes beyond use for dispatch via ECRF	This document

10.6 "urn:emergency:service:responder.police" Registry

IANA is requested to add the following values to the urn:emergency:service:responder.police registry

Name	Description	Reference
federal	An appropriate federal agency (subregistry defined below)	This document
stateProvincial	State or provincial police office	This document
tribal	Native American police (reservation)	This document
countyParish	County or Parish police (not Sheriff)	This document
sheriff	Sheriff's office, when both a police and Sheriff dispatch may be possible	This document
local	City, Town, Township, Borough or Village police	This document

10.7 "police.federal" Registry

IANA is requested to add the following values to the urn:emergency:service:responder.police.federal registry

Name	Full Name	Reference
fbi	Federal Bureau of Investigation	This document
rcmp	Royal Canadian Mounted Police	This document
usss	U.S. Secret Service	This document
dea	Drug Enforcement Agency	This document
marshal	Marshals Service	This document
cbp	Customs and Border Protection	This document
ice	Immigration and Customs Enforcement	This document
atf	Bureau of Alcohol, Tobacco, Firearms and Explosives	This document
pp	U.S. Park Police	This document
dss	Diplomatic Security Service	This document
fps	Federal Protective Service	This document
military	Used for military installations	This document

© Copyright 2011-2022 National Emergency Number Association, Inc.

10.8 "urn:emergency:service:responder.fire" Registry

IANA is requested to add the following values to the urn:emergency:service:responder.fire registry

Name	Description	Reference
forest	Forest Fire Service	This document
airport	Airort Fire Service	This document
military	Used for military installations	This document
private	Private Fire Service	This document

10.9 "urn:emergency:service:responder.ems" Registry

IANA is requested to add the following values to the urn:emergency:service:responder.ems registry

Name	Description	Reference
tribal	Native American EMS (reservation)	This document
countyParish	County or Parish EMS	This document
local	City, Town, Township, Borough or Village EMS	This document
private	Contracted Ambulance Service	This document
military	Used for military installations	This document

10.10 "urn:emergency:uid" Registry

IANA is requested to add the following values to the urn:emergency:uid registry

Name	Purpose	Reference
callid	Call Tracking Identifier	This document
incidentid	Incident Tracking Identifier	This document
logid	LogEvent Identifier	This document
lostsrc	LoST Source Identifier	This document
lostQuery	LoST Query Identifier	This document
queryd	Query identifier (links a response to its query	This document
subid	Subscription identifier (links a SUBSCRIBEs/RESPONSEs)	This document

10.11 "serviceNames" Registry

IANA is requested to add the following values to the serviceNames registry

Service Name	Service	Reference
ADR	Additional Data Repository (if hosted on an ESInet)	This document

© Copyright 2011-2022 National Emergency Number Association, Inc.

Bridge	Bridge	This document
ECRF	Emergency Call Routing Function	This document
ESRP	Emergency Service Routing Proxy	This document
GCS	Geocode Conversion Service	This document
IMR	Interactive Media Response Service	This document
Logging	Logging Service	This document
LVF	Location Validation Function	This document
MCS	MSAG Conversion Service	This document
MDS	Mapping Data Service	This document
PolicyStore	Policy Store	This document
PSAP	PSAP	This document
SAL	Service/Agency Locator	This document

10.12 "serviceState" Registry

IANA is requested to add the following values to the serviceState registry

Name	Description	Reference
Normal	The service is operating normally. Calls can be sent to this destination normally.	This document
Unstaffed	(applies to PSAPs only) The PSAP has indicated that it is not currently answering calls. Calls must be sent to another destination.	This document
ScheduledMaintenanceDown	The service is undergoing maintenance activities and is not accepting service requests. Calls must be sent to another destination.	This document
ScheduledMaintenanceAvailable	The service is undergoing maintenance activities, but will respond to service requests, possibly with reduced availability. Calls can be sent to this destination normally.	This document
MajorIncidentInProgress	The element is operating normally but is handling a major incident and may be unable to accept some requests. Calls could be sent to this destination	This document

© Copyright 2011-2022 National Emergency Number Association, Inc.

Name	Description	Reference
	but doing so may precipitate that destination into an overloaded state.	
Partial	Processing some requests, but response may be delayed. Calls could be sent to this destination.	This document
Overloaded	The service is completely overloaded. Calls must be sent to another destination.	This document
GoingDown	The service is being taken out of service. Calls must be sent to another destination.	This document
Down	The service is unavailable. Calls must be sent to another destination.	This document
Unreachable	Subscriber is unable to contact the service.	This document

10.13 "elementState" Registry

IANA is requested to add the following values to the elementState registry

Name	Description	Reference
Normal	The element is operating normally	This document
ScheduledMaintenance	The element is undergoing maintenance activities and is not processing requests	This document
ServiceDisruption	The element has significant problems and is unable to process all requests	This document
Overloaded	The element is completely overloaded	This document
GoingDown	The element is being taken out of service	This document
Down	The element is unavailable	This document
Unreachable	Subscriber is unable to contact the service	This document

10.14 "urn:emergency:service:serviceagencyLocator" Registry

IANA is requested to add the following values to the urn:emergency:service:serviceagencylocator registry:

© Copyright 2011-2022 National Emergency Number Association, Inc.

Service Identifier	Service	Reference
ADR	Additional Data Repository (if hosted on an ESInet)	This document
Bridge	Bridge	This document
BCF	Border Control Function	This document
ECRF	Emergency Call Routing Function	This document
ESRP	Emergency Service Routing Proxy	This document
GCS	Geocode Conversion Service	This document
IMR	Interactive Media Response Service	This document
Logging	Logging Service	This document
LVF	Location Validation Function	This document
MCS	MSAG Conversion Service	This document
MDS	Mapping Data Service	This document
PolicyStore	Policy Store	This document
PSAP	PSAP	This document
SAL	Service/Agency Locator	This document

10.15 "SIPheaderIsOperatorConditions" Registry

IANA is requested to add the following values to the SIPheaderIsOperatorCondition registry

Name	Description	Reference
present	The header field is present	This document
missing	The header field is not present	This document
badSyntax	The header field is syntactically incorrect	This document
erroneous	The header field contains syntactically correct but erroneous contact	This document

10.16 "urn:emergency:media-feature" Registry

IANA is requested to add the following values to the urn:emergency:media-feature registry:

Tag	Purpose	Reference
psap-call-control	UA can support Call Party Hold per Appendix C	This document
tty-interworking	UA supports TTY interworking	This document

© Copyright 2011-2022 National Emergency Number Association, Inc.

10.17 "queueState" Registry

IANA is requested to add the following values to the queueState registry:

Name	Description	Reference
Active	One or more entities are actively available or are currently handling calls being enqueued	This document
Inactive	No entity is available or actively handling calls being enqueued	This document
Disabled	The queue is disabled by management action and no calls may be enqueued	This document
Full	The queue is full, and no new calls can be enqueued on it	This document
Standby	The queue has one or more entities that are available to take calls, but the queue is not presently in use. When a call is enqueued, the state changes to "Active"	This document
ResourceExhausted	The downstream entity cannot accept any more calls for a reason other than one of the above conditions.	This document
Unreachable	The queue is unreachable. Used by the subscriber to provide a value when it is unable to subscribe.	This document

10.18 "securityPosture" Registry

IANA is requested to add the following entries to the securityPosture registry:

Value	Purpose	Reference
Green	The entity is operating normally. Calls can be sent to this destination normally.	This document
Yellow	The entity is receiving suspicious activity but is able to operate normally. Calls could be sent to this destination.	This document
Orange	The entity is receiving fraudulent calls/events, is stressed, but is able to continue most operations. Calls could be sent to this destination but doing so may precipitate that destination into an overloaded state.	This document
Red	The entity is under active attack and is overwhelmed. Calls must be sent to another destination.	This document

© Copyright 2011-2022 National Emergency Number Association, Inc.

10.19 "ESRP Notify Event Code" Registry

IANA is requested to add the following entries to the EsrpNotifyEventCode registry:

Value	Purpose	Category	Reference
Normal	A normal route action was performed. This is a courtesy notification	Safety	This document
Default	There was insufficient location information to determine the next hop, a default location was used for routing	Safety	This document
Congestion	The normal route was congested; an alternate route was taken	Safety	This document
Disaster	The normal destination is in disaster mode and this call was diverted	Safety	This document
IMR	The call met the conditions for diversion to an IMR (Interactive Media Response)	Safety	This document
Busy	There were no routes available and busy was returned for this call	Safety	This document
Error	The ESRP encountered an error and a default route was taken	Safety	This document
Fatal Error	The ESRP encountered a fatal error that caused the call to fail (i.e., got a 600 Busy Everywhere response)	Safety	This document
TimeOfDay	An alternate PSAP handles calls in off hours	Safety	This document
GenericPolicy	Diversion occurred because of policy, not covered above	Safety	This document
Test	This is a test call	Safety	This document

10.20 "Route Cause" Registry

IANA is requested to add the following entries to the RouteCause registry:

Value	Code	Text	Reference
Normal-NextHop	200	Normal Next Hop	This document
TimeOfDay	401	Time of Day	This document
Congestion	402	Congestion	This document
Disaster	403	Disaster	This document
IMR	404	Interactive Media Response	This document
GenericPolicy	405	Policy decision not covered above	This document

© Copyright 2011-2022 National Emergency Number Association, Inc.

Value	Code	Text	Reference
Default	406	Default with no/bad location	This document

10.21 "LogEvent" Registry

IANA is requested to add the following entries to the LogEvent registry:

Value	Purpose	Reference
CallProcessLogEvent	Logged by an FE that is not call stateful, to denote its handling of a call.	This document
CallStartLogEvent	Logged by an FE that is call stateful, when it begins processing a call.	This document
CallEndLogEvent	Logged by an element that is call stateful, when its processing of a call ends.	This document
RecCallStartLogEvent	RecCallStartEvent is identical to CallStartEvent, but is logged by the Logging Service (SRS) and the client (SRC) to denote the beginning of a SIPREC recording session.	This document
RecCallEndLogEvent	RecCallEndEvent is identical to CallEndEvent, but is logged by the Logging Service (SRS) and the client (SRC) to denote the end of a SIPREC recording session.	This document
CallTransferLogEvent	Logged by an FE when it transfers a call.	This document
RouteLogEvent	Logged by Proxy Servers (e.g., ESRPs) to denote the route selected and the rule or reason that caused the route to be selected.	This document
MediaStartLogEvent	Logged by an FE that anchors media, to denote the start of a given call medium. Includes the SDP that describes the medium.	This document
MediaEndLogEvent	Logged by an FE that anchors media, to denote end of a medium. Includes the specific media label from the SDP which describes the medium that has ended.	This document
RecMediaStartLogEvent	RecMediaStartEvent is identical to MediaStartEvent but is logged by the SRS and SRC to denote the start of a medium in a SIPREC recording session.	This document

© Copyright 2011-2022 National Emergency Number Association, Inc.

Value	Purpose	Reference
RecMediaEndLogEvent	RecMediaEndEvent is identical to MediaEndEvent but is logged by the SRS and SRC to denote the end of a medium in a SIPREC recording session.	This document
RecordingFailedLogEvent	Logged by an SRC or SRS when its attempt to record media via a SIPREC session fails.	This document
MessageLogEvent	Logged by an FE when it handles a SIP MESSAGE request.	This document
AdditionalAgencyLogEvent	Logged by an FE when it is discovered that another agency may be involved in an Incident.	This document
IncidentMergeLogEvent	Logged by an FE to denote that this is an additional call about an Incident that is already being handled, effectively assigning the call to the existing Incident.	This document
IncidentUnMergeLogEvent	Logged by an FE to counteract a IncidentMergeEvent that it previously logged.	This document
IncidentSplitLogEvent	Logged by an FE when it creates a new Incident by "cloning" (copying the data from) an existing Incident.	This document
IncidentLinkLogEvent	Logged by an FE to associate an Incident with another Incident, when the two Incidents are somehow related but are not the same Incident.	This document
IncidentUnLinkLogEvent	Logged by an FE to counteract a IncidentLinkEvent that it previously logged.	This document
IncidentClearLogEvent	When an agency finishes its handling of an Incident, the responsible FE logs an IncidentClearEvent record. Other agencies may still be processing the Incident.	This document
IncidentReopenLogEvent	If an agency needs to log new events on an Incident for which it has previously logged an IncidentClearEvent, the responsible FE logs an IncidentReopenEvent.	This document
LostQueryLogEvent	Logged by an FE that sends or receives a LoST query. Includes a unique "LostQueryId" that will be returned in the response to allow matching the query to the response.	This document
LostResponseLogEvent	Logged by an FE when it sends or receives a LoST response. Includes the "LostQueryId" that was	This document

© Copyright 2011-2022 National Emergency Number Association, Inc.

Value	Purpose	Reference
	included in the corresponding LoST query, to allow matching the response to the query.	
CallSignalingMessageLogEvent	An FE logs call signaling messages (e.g., SIP requests and responses) that it sends or receives.	This document
SiprecMetadataLogEvent	Used by the Logging Service to log any SIPREC metadata it receives from the SRC.	This document
NonRtpMediaMessageLogEvent	Used by the Logging Service to log media that do not use RTP for transport.	This document
AliLocationQueryLogEvent	Used by an LSRG to log an ALI query it sends or receives. Includes a unique "AliLocationQueryId" that will be returned in the response to allow matching the query to the response.	This document
AliLocationResponseLogEvent	Used by an LSRG to log an ALI response it sends or receives. Includes the "AliLocationQueryId" that was included in the corresponding ALI query, to allow matching the response to the query.	This document
MalformedMessageLogEvent	Used by an FE to log a malformed SIP request it received.	This document
EidoLogEvent	Logged by an FE that sends or receives an Emergency Incident Data Object (EIDO), or a reference to an EIDO.	This document
DiscrepancyReportLogEvent	Logged by an FE that sends or receives a Discrepancy Report (DR) or an update to a DR (Status, Resolution, etc.).	This document
ElementStateChangeLogEvent	Logged by an FE to denote a change to one of the states listed in the elementState registry.	This document
ServiceStateChangeLogEvent	Logged by a Service to denote a change to one of the states listed in the serviceState.	This document
AdditionalDataQueryLogEvent	Used by an FE to log an Additional Data query it sends or receives. Includes an "AdditionalDataQueryId" used to match the query to its response.	This document
AdditionalDataResponseLogEvent	Used by an FE to log an Additional Data response it sends or receives. Includes the "AdditionalDataQueryId" from the original query, which is used to match the response to its query.	This document
LocationQueryLogEvent	Used by an FE to log a HELD dereference or SIP SUBSCRIBE request for location data. Includes a	This document

© Copyright 2011-2022 National Emergency Number Association, Inc.

Value	Purpose	Reference
	"LocationQueryId" used to match the dereference or subscription to its response.	
LocationResponseLogEvent	Used by an FE to log a HELD response or a SIP NOTIFY with location. Includes the "LocationQueryId" from the original query or SUBSCRIBE, which is used to match the response to its dereference or query.	This document
CallStateChangeLogEvent	Used by an FE to log a call state change to one of the states listed in the CallStates registry.	This document
GatewayCallLogEvent	Used by an LNG, LPG, or LSRG to log a call entering or leaving it on a legacy interface.	This document
HookflashLogEvent	An LPG logs the HookflashEvent when a "hookflash" is detected on a legacy interface.	This document
LegacyDigitsLogEvent	Used by an LPG to log DTMF or MF digits received or generated on a legacy interface.	This document
AgentStateChangeLogEvent	Used by an FE to log an Agent state change to one of the states in the AgentStates registry in the IANA registry.	This document
QueueStateChangeLogEvent	Logged by an FE that manages a queue to denote a change in state to one of the states listed in the QueueState registry.	This document
KeepAliveFailureLogEvent	Used by an FE to log a malformed, invalid, or timed-out response for an OPTIONS request it sent to another FE or Service.	This document
RouteRuleMsgLogEvent	Logs the "log" element from the Route Policy Syntax containing details on the given rule set.	This document
PolicyChangeLogEvent	An FE logs the PolicyChangeEvent when a policy is created, updated, or deleted.	This document
VersionsLogEvent	Used by an FE to log the response it receives for a Versions request it issued to a web service on an initial request or when the response has changed.	This document
SubscribeLogEvent	Logs subscription requests for any defined Event Package.	This document

10.22 "LogEvent Protocol" Registry

IANA is requested to add the following entries to the LogEventProtocol registry:

© Copyright 2011-2022 National Emergency Number Association, Inc.

Name	Reference
SIP	RFC3261
MSRP	RFC4975

10.23 "LogEvent CallTypes" Registry

IANA is requested to add the following entries to the LogEvent CallTypes registry:

Name	Description	Classification
emergency	Call is deemed urgent call and treated as such	Primary
nonEmergency	Call is not deemed urgent	Primary
silentMonitoring	Silently monitor the activities of the target	Primary
intervene	Intervene on the activities of the target	Primary
legacyWireline	Call from a wireline device received from a legacy network	Secondary
legacyWireless	Call from a wireless device received from a legacy network	Secondary
legacyVoip	Call from a VoIP device received from a legacy network	Secondary

10.24 "Call States" Registry

IANA is requested to add the following entries to the CallStates registry:

Name	Description
callBegin	Indicates the start of a new call. If the call is also a SIP call, the CallStart LogEvent must be logged. "CallStateLegCallId" must not be supplied as no third leg is involved. "CallStateTargetID" must either be the address of the destination target (in the case of a call being originated) or the address of the originator (in the case the call is being received)
callAlerting	A notification of the call is being presented. "CallStateLegCallId" and "CallStateTargetID" must not be supplied.
callQueued	A call is on a queue to be answered. "CallStateLegCallId" must not be supplied; "CallStateTargetID" must be the name of the queue.
callAnswered	Indicates that the call has been answered. "CallStateTargetID" may indicate the device used to answer the call (not the agent, agentID is for that purpose). "CallStateLegCallId" must not be supplied.
callEnd	Indicates the end of a call. If the call is also a SIP call, the CallEnd LogEvent must be logged. "CallStateLegCallId" and "CallStateTargetID" must not be supplied.

© Copyright 2011-2022 National Emergency Number Association, Inc.

Name	Description
callCancel	A cancel request has been received for the call. "CallStateLegCallId" and "CallStateTargetID" must not be supplied.
callHold	Indicates that the call has been put on hold for later retrieval. If the use of an external device such as a Music-on-Hold server is used, the "CallStateLegCallId" should contain the identifier of that call leg and "CallStateTargetID" may contain its identity.
callPark	Indicates that the call has been parked for later retrieval. "CallStateTargetID" must contain the park identifier orbit that was used. If an external device is used, the "CallStateLegCallId" should contain the identifier of that call leg.
callRetrieve	Indicates that a held or parked call has been re-activated. "CallStateLegCallId" and "CallStateTargetID" must not be supplied.
partyAdd	Indicates that the addition of a party to the call is being requested (thus creating a conference in the case there was only two parties). "CallStateTargetID" must specify the identity of the party being added and "CallStateLegCallId" must specify the identifier of the call leg used to contact the party. This LogEvent must be generated at the beginning of the attempt to add a party. The outcome of the attempt is determined by the events related to the call leg specified by "CallStateLegCallId".
partyRemove	Indicates that a party has been removed from a conference (either by user request or by loss of call leg). "CallStateTargetID" must specify the identity of the party removed. "CallStateLegCallId" must not be supplied.
callBargeIn	Indicates that an outside party requests to join an active call. For the originator of the barge in request, "CallStateLegCallId" specifies the identity of the call to be joined. For the recipient of the barge in request, "CallStateLegCallId" specifies the identity of the call leg to be added to the active call. The outcome of the barge in request is determined by the events related to the call leg barging into the active call.

10.25 "LogEvent Announcement Types" Registry

IANA is requested to add the following entries to the LogEventAnnoucementTypes registry:

Name	Description
AutoAnswerGreeting	Indicates an announcement played automatically after a call is answered by an agent. Typically recorded with the agent's voice, this type of recorded greeting is used to standardize the answering of calls.

© Copyright 2011-2022 National Emergency Number Association, Inc.

Name	Description
NoAgentsAvailableAnnouncement	Indicates an announcement indicating no agents are currently available to take the call and the call will be answered by the next available agent.
StandardAnnouncement	Indicates an announcement played to all calls regardless of the availability of agents to take the call.

10.26 "Non-RTP Media Types" Registry

IANA is requested to add the following entries to the nonRTPmediaTypes registry:

Name	Description
MSRP	Media Session Relay Protocol

10.27 "Agency Roles" Registry

IANA is requested to add the following entries to the AgencyRoles registry:

Role	Description	Reference
PSAP	Per NENA ADM-000 Master Glossary: "… responsible for receiving 9-1-1 calls and processing those calls according to a specific operational policy."	This document
Dispatch	Per ANS1.107.1.2015: "… alerting and directing the response of public safety responders to the desired location".	This document
911 Authority	Per NENA ADM-000 Master Glossary: "… governmental entity responsible for 9-1-1 service operations.	This document
ESInet Service Provider	The entity responsible for the operation of an Emergency Services IP Network.	This document
ESRP Service Provider	The entity responsible for the operation of an Emergency Service Routing Proxy	This document
ECRF/LVF Service Provider	The entity responsible for the operation of an Emergency Call Routing Function/Location Validation Function.	This document
LIS Service Provider	The entity responsible for the operation of a Location Information Server.	This document

© Copyright 2011-2022 National Emergency Number Association, Inc.

Role	Description	Reference
National	Agency Role modifier are scopes that can be applied to the above agency roles to further clarify the extent of the authority.	This document
State	Agency Role modifier are scopes that can be applied to the above agency roles to further clarify the extent of the authority.	This document
Regional	Agency Role modifier are scopes that can be applied to the above agency roles to further clarify the extent of the authority.	This document
Local	Agency Role modifier are scopes that can be applied to the above agency roles to further clarify the extent of the authority.	This document

10.28 "Agent Roles" Registry

IANA is requested to add the following entries to the AgentRoles registry:

Role	Description	Reference
Dispatching	Per ANS1.107.1.2015: "… alerting and directing the response of public safety responders to the desired location".	This document
Call Taking	Per ANS1.107.1.2015: "… processes incoming calls through the analyzing, prioritizing, and disseminating of information to aid in the safety of the public and responders".	This document
GIS Analysis	assembles and maintains geospatial and addressing information.	This document
IP Network Administration	monitors, manages and controls network elements and services (e.g., switches, routers, gateways, firewalls and network services such as DNS and DHCP); plans for and responds to service outages and other problems.	This document
Database Administration	installs, configures, manages, monitors and controls access to databases.	This document
IT Systems Administration	installs, configures, supports and maintains system hardware, operating systems, application elements and services; plans for and responds to service outages and other problems.	This document

© Copyright 2011-2022 National Emergency Number Association, Inc.

Role	Description	Reference
Application Administration	installs, configures, supports and maintains applications; plans for and responds to service outages and other problems.	This document
Security Administration	creates, assigns, configures, maintains and supports user authentication and authorization elements and services; monitors for possible security violations and vulnerabilities, and ensures that vulnerabilities are corrected.	This document
Records Production	searches, retrieves and reproduces records and recordings for internal and external uses, including FOIA requests, subpoenas, and media requests.	This document
Data Analysis	researches and analyzes specific kinds of data to identify trends, anomalies and conditions important to supporting emergency services.	This document
Quality Assurance Evaluation	Per ANS1.107.1.2015: "… reviews telecommunicator work performance and documents an evaluation of the level of compliance with Agency directives and standards."	This document
Management	Role Modifier (may be added to further specify the above roles).	This document
Supervisor	Role Modifier (may be added to further specify the above roles).	This document
Trainer	Role Modifier (may be added to further specify the above roles).	This document
Trainee	Role Modifier (may be added to further specify the above roles).	This document
Assist Manager	Role Modifier (may be added to further specify the above roles).	This document
Shift Supervisor	oversees individuals who perform the Roles of Dispatching, Call Taking or a combination of both.	This document
GIS Specialist	plans, develops, and implements systems and databases for storing and accessing geospatial data.	This document
GIS Supervisor	oversees individuals who perform the Role of GIS Specialist.	This document

© Copyright 2011-2022 National Emergency Number Association, Inc.

Role	Description	Reference
Maintenance Supervisor	oversees individuals who perform the Role of Maintenance Technician.	This document
Maintenance Technician	responsible for performing general maintenance and repairs on equipment and assets, assists with the installation of equipment and manages the upkeep of tools, equipment and machinery.	This document
Temporary Technician	on a short-term basis, responsible for performing general maintenance and repairs on equipment and assets, assists with the installation of equipment and manages the upkeep of tools, equipment and machinery.	This document
ESInet Network Operator	monitors and troubleshoots communication and application-related issues through the use of management and diagnostic tools for an Emergency Services IP Network.	This document
ESInet Network Operations Supervisor	oversees individuals who perform Role of ESInet Network Operator.	This document
911 Authority Director	controls the management and operation of a 911 Authority.	This document
911 Authority Agent	performs duties related to the operation of a 911 Authority.	This document
Database Administrator	uses specialized software to store and organize data, ensuring that data are available to users and secure from unauthorized access.	This document
IT Systems Analyst	uses analysis and design techniques to solve business problems using information technology	This document
Records Production Specialist	organizes and manages information data by ensuring that it maintains its quality, accuracy, accessibility, and security in both paper files and electronic systems.	This document

10.29 "Status Codes" Registry

IANA is requested to add the following entries to the StatusCodes registry:

Status Code	Description	Reference
333	Iterative Refer	This document
433	No such sourceId	This document

© Copyright 2011-2022 National Emergency Number Association, Inc.

Status Code	Description	Reference
434	Signature Verification Failure	This document
436	Duplicate or Invalid Priority	This document
437	Bad Policy Structure	This document
438	Unacceptable Algorithm	This document
441	Index beyond available names	This document
442	Unacceptable Parameters	This document
451	Unknown or bad Policy Name	This document
452	Unknown or bad Agency Name	This document
453	Not available here, no referral available	This document
454	Unspecified Error	This document
456	Bad queue	This document
457	Bad dequeuePreference	This document
458	Policy Violation	This document
459	Bad PolicyExpirationTime	This document
460	Bad LogEvent	This document
461	LogEvent too big	This document
462	LogEvent extension not on allowed list	This document
463	LogEvent extension on disallowed list	This document
464	No Text in this Call	This document
465	Bad Timestamp	This document
466	EndTime occurs before StartTime	This document
467	Bad or missing Geoshape	This document
469	Unknown MCS/GCS	This document
470	Unknown Service/Database ("not ours")	This document
471	Unauthorized Reporter	This document
472	Unauthorized Responder	This document
473	Unknown ReportId	This document
474	Resolution already provided	This document
475	Response not available yet	This document

10.30 "Interface Names" Registry

IANA is requested to add the following entries to the Interface Names registry:

Name	Reference
SIPcall	This document
LoST	This document
ElementState	This document

© Copyright 2011-2022 National Emergency Number Association, Inc.

Name	Reference
ServiceState	This document
HELDdereference	This document
SIMPLEpresence	This document
PolicyStore	This document
DiscrepancyReport	This document
QueueState	This document
DequeueRegistration	This document
ESRPNotify	This document
AbandonedCall	This document
SI	This document
GapOverlap	This document
PIDFLOtoMSAG	This document
Geocode	This document
ReverseGeocode	This document
ConferenceEvent	This document
Logging	This document
SIPREC	This document
LoggingRetrieval	This document
AgencyLocatorDereference	This document
AgencyLocatorNameSearch	This document
MapDatabase	This document
LNGadr	This document

10.31 "Match Type" Registry

IANA is requested to add the following entries to the Match Type registry:

Token	Description
Address	A datum representing a site, structure, or portion of a structure having a specific address.
RoadCenterline	A datum representing a road centerline, which may be associated with one or more ranges of addresses.
PoliticalBoundary	A datum representing a political subdivision, typically designated with country and one or more of A1, A2, A3, A4, and/or A5 (civic address elements).
MsagCommunity	A datum representing a legacy MSAG community. There is no defined method for routing by MSAG community in this document.

© Copyright 2011-2022 National Emergency Number Association, Inc.

Token	Description
CoverageRegion	A datum used by a LoST server to define an area for which it can authoritatively answer queries.
Hybrid	Any combination of data that spans multiple layers or categories.
Other	Any source of data which is not otherwise defined in this registry.

10.32 "GIS Data Layers" Registry

IANA is requested to add the following entries to the GIS Data Layers registry:

Name	Reference
RoadCenterLine	This document
SiteStructurePoint	This document
PsapPolygon	This document
PolicePolygon	This document
FirePolygon	This document
FireForestPolygon	This document
FireAirportPolygon	This document
FireMilitaryPolygon	This document
FirePrivatePolygon	This document
EmsPolygon	This document
EmsPrivatePolygon	This document
EmsAirPolygon	This document
EmsMilitaryPolygon	This document
PoisonControlPolygon	This document
MountainRescuePolygon	This document
CoastGuardPolygon	This document
PoliceCountyPolygon	This document
PoliceStateProvincialPolygon	This document
PoliceFederalPolygon	This document
PoliceFederalFbiPolygon	This document
PoliceFederalRcmpPolygon	This document
PoliceFederalSecretServicePolygon	This document
PoliceFederalDeaPolygon	This document
PoliceFederalMarshalPolygon	This document
PoliceFederalCustomsBorderProtectionPolygon	This document
PoliceFederalImmigrationCustomsPolygon	This document
PoliceFederalAtfPolygon	This document

© Copyright 2011-2022 National Emergency Number Association, Inc.

Name	Reference
PoliceFederalParkPolygon	This document
PoliceFederalDiplomaticSecurityPolygon	This document
PoliceFederalProtectiveServicePolygon	This document
PoliceSheriffPolygon	This document
PoliceMilitaryPolygon	This document
PoliceCampusPolygon	This document
PolicePrivatePolygon	This document
PoliceAirportPolygon	This document
PoliceHousingPolygon	This document
PoliceParkPolygon	This document
StreetNameAliasTable	This document
LandmarkNamePartTable	This document
LandmarkNameCompleteAliasTable	This document
A1Polygon	This document
A2Polygon	This document
A3Polygon	This document
A4Polygon	This document
A5Polygon	This document
RailroadCenterLine	This document
HydrologyLine	This document
HydrologyPolygon	This document
CellSectorPoint	This document
LocationMarkerPoint	This document

10.33 "Policy Type" Registry

IANA is requested to add the following entries to the Policy Type registry:

Type	Format	Use	Reference
OriginationRoutePolicy	PRR	Policy Routing Rules for incoming queue	This document
NormalNextHopRoutePolicy	PRR	Policy Routing Rules for Normal Next Hop	This document
OtherRoutePolicy	PRR	Policy Routing Rules for common policies	This document

© Copyright 2011-2022 National Emergency Number Association, Inc.

Type	Format	Use	Reference
DequeueExpirationTime	XACML	How long subscriptions to DequeueRegistration are allowed	This document
GISReplicas	XACML	Which entities are allowed to maintain replicas of GIS data	This document
ECRF-LVFreplica	XACML	Which entities are allowed to maintain replicas of ECRF/LVF data	This document
TestCalls	XACML	Which originators may process PRR test calls	This document
SIPcall	XACML	Access rights for a SIP Call Interface.	This document
LoST	XACML	Access rights for a LoST Interface	This document
ElementState	XACML	Access rights for ElementState subscription	This document
ServiceState	XACML	Access rights for ServiceState subscription	This document
HELDdereference	XACML	Access rights for HELD dereference interface	This document
AgentPresencePublish	XACML	Access rights for presence (sip) PUBLISH interface	This document
AgentPresencePut	XACML	Access rights for presence (http) status change interface	This document
AgentPresenceSubscribe	XACML	Access rights for presence subscription	This document
PolicyStore	XACML	Access rights for Policy Store interface	This document
DiscrepancyReport	XACML	Access rights for Discrepancy Report interface	This document
QueueState	XACML	Access rights for QueueState subscription	This document
DequeueRegistration	XACML	Access rights for DequeueRegistration interface	This document

© Copyright 2011-2022 National Emergency Number Association, Inc.

Type	Format	Use	Reference
ESRPNotify	XACML	Access rights for ESRP Notify subscription	This document
AbandonedCall	XACML	Access rights for AbandonedCall subscription	This document
SpatialInterface	XACML	Access rights for Spatial Interface	This document
GapOverlap	XACML	Access rights for GapOverlap subscription	This document
MCS	XACML	Access rights for MCS interface	This document
GCS	XACML	Access rights for GCS interface	This document
ConferenceEvent	XACML	Access rights for ConferenceEvent subscription	This document
LoggingService	XACML	Access rights for Logging Service interface	This document
LoggingSIPREC	XACML	Access rights for Logging Service SIPREC interface	This document
ServiceAgencyLocatorDereference	XACML	Access rights for S/A L dereference interface	This document
ServiceAgencyLocatorNameSearch	XACML	Access rights for S/A L name search interface	This document
ServiceAgencyLocatorIndex	XACML	Access rights for S/A L Locator Index interface	This document
MapDatabase	XACML	Access rights for Map Database interface	This document

10.34 "Discrepancy Report Status Token" Registry

IANA is requested to add the following entries to the DiscrepancyReportStatusToken registry:

Token	Name	DiscrepancyReports	Reference
AbleDelete	Problem	PermissionsDiscrepancyReport	This document
AbleRead	Problem	PermissionsDiscrepancyReport	This document
AbleSubscribe	Problem	PermissionsDiscrepancyReport	This document
AbleWrite	Problem	PermissionsDiscrepancyReport	This document

© Copyright 2011-2022 National Emergency Number Association, Inc.

Token	Name	DiscrepancyReports	Reference
AddressRange	Problem	GISDiscrepancyReport	This document
BadAdditionalData	Problem	OriginatingServiceDiscrepancyReport	This document
BadCDR	Problem	BCFDiscrepancyReport	This document
BadCertificateChain	Problem	PermissionsDiscrepancyReport	This document
BadGeometry	Problem	GISDiscrepancyReport	This document
BadPIDFLO	Problem	LISDiscrepancyReport, OriginatingServiceDiscrepancyReport	This document
BadSDP	Problem	BCFDiscrepancyReport	This document
BadSIP	Problem	OriginatingServiceDiscrepancyReport	This document
BelievedInvalid	Problem	LoSTDiscrepancyReport	This document
BelievedValid	Problem	LoSTDiscrepancyReport	This document
CallDropped	Problem	OriginatingServiceDiscrepancyReport	This document
CallDrought	Problem	ESRPDiscrepancyReport, OriginatingServiceDiscrepancyReport	This document
CallFlood	Problem	OriginatingServiceDiscrepancyReport	This document
CallReceived	Problem	ESRPDiscrepancyReport	This document
CallTakerAdvised	Validation Response	CallTakerDiscrepancyResponse	This document
CallTransferIncorrect	Problem	IMRDiscrepancyReport	This document
ConflictingRoute	Problem	PolicyDiscrepancyReport	This document
Critical	Severity	DiscrepancyReportRequest	This document
DataCorrected	Validation Response	GISDiscrepancyResponse	This document
DataExpired	Problem	LoSTDiscrepancyReport	This document
Degraded	Severity	DiscrepancyReportRequest	This document
DeviceConfigError	Validation Response	LISDiscrepancyResponse	This document
DiscrepancyCorrected	Validation Response	LoSTDiscrepancyResponse, BCFDiscrepancyReport, LoggingDiscrepancyResponse, SIPDiscrepancyResponse, PermissionsDiscrepancyResponse	This document
DiscrepancyNotFound	Validation Response	LoSTDiscrepancyResponse, BCFDiscrepancyReport	This document
DisplayData	Problem	GISDiscrepancyReport	This document
DuplicateAttribute	Problem	GISDiscrepancyReport	This document

© Copyright 2011-2022 National Emergency Number Association, Inc.

Token	Name	DiscrepancyReports	Reference
EngorgedQ	Problem	ESRPDiscrepancyReport, IMRDiscrepancyReport, SIPDiscrepancyReport	This document
EntryAdded	Validation Response	LoSTDiscrepancyResponse	This document
ExcessiveSilence	Problem	IMRDiscrepancyReport	This document
FALSE	LocationCorrect	OriginatingServiceDiscrepancyReport	This document
findService	Query	LoSTDiscrepancyReport	This document
Firewall	Problem	BCFDiscrepancyReport	This document
Gap	Problem	GISDiscrepancyReport	This document
GeneralProvisioning	Problem	GISDiscrepancyReport	This document
getServiceBoundary	Query	LoSTDiscrepancyReport	This document
GIS	Validation Response	ESRPDiscrepancyResponse	This document
Impaired	Severity	DiscrepancyReportRequest	This document
IncorrectDataType	Problem	GISDiscrepancyReport	This document
IncorrectDHCP	Problem	NetworkDiscrepancyReport	This document
IncorrectDNS	Problem	NetworkDiscrepancyReport	This document
IncorrectLocation	Problem	LISDiscrepancyReport, OriginatingServiceDiscrepancyReport	This document
IncorrectLoST	Problem	GISDiscrepancyReport	This document
IncorrectRecords	Problem	LISDiscrepancyReport	This document
IncorrectURI	Problem	LoSTDiscrepancyReport	This document
IncorrectURN	Problem	PolicyDiscrepancyReport	This document
InitialINVITE	Problem	PSAPDiscrepancyReport	This document
InitialTrafficBlocked	Problem	BCFDiscrepancyReport	This document
InputFailed	Problem	IMRDiscrepancyReport	This document
InsufficientCredentials	Validation Response	PolicyStoreDiscrepancyResponse	This document
InvalidADR	Problem	OriginatingServiceDiscrepancyReport	This document
InvalidRecord	Validation Response	OriginatingServiceDiscrepancyResponse	This document
InvalidURN	Problem	PolicyDiscrepancyReport	This document
InviteSRSerror	Problem	LoggingDiscrepancyReport	This document
listServices	Query	LoSTDiscrepancyReport	This document
listServicesByLocation	Query	LoSTDiscrepancyReport	This document

© Copyright 2011-2022 National Emergency Number Association, Inc.

Token	Name	DiscrepancyReports	Reference
LocationErrorInError	Problem	LoSTDiscrepancyReport	This document
LocationMissing	Problem	OriginatingServiceDiscrepancyReport	This document
LocationNotLVFValid	Problem	OriginatingServiceDiscrepancyReport	This document
LocationNotUsable	Problem	OriginatingServiceDiscrepancyReport	This document
LocationReferenceNotResolved	Problem	LISDiscrepancyReport	This document
LogEventError	Problem	LoggingDiscrepancyReport	This document
Loop	Problem	PolicyDiscrepancyReport	This document
Malformed	Problem	ADRDiscrepancyReport PolicyDiscrepancyReport	This document
MalformedURI	Problem	GISDiscrepancyReport	This document
MediaLoss	Problem	BCFDiscrepancyReport	This document
MediaProblem	Problem	SIPDiscrepancyReport	This document
MESSAGE	Problem	SIPDiscrepancyReport	This document
MidDialog	Problem	SIPDiscrepancyReport	This document
MidTrafficBlocked	Problem	BCFDiscrepancyReport	This document
Minor	Severity	DiscrepancyReportRequest	This document
Moderate	Severity	DiscrepancyReportRequest	This document
MSAGtoPIDFLO	ServiceCall	MCSDiscrepancyReport	This document
MultipleMappings	Problem	LoSTDiscrepancyResport	This document
NoANI	Problem	OriginatingServiceDiscrepancyReport	This document

© Copyright 2011-2022 National Emergency Number Association, Inc.

Token	Name	DiscrepancyReports	Reference
NoDiscrepancy	Validation Response	ADRDiscrepancyResponse, BCFDiscrepancyResponse, CallTakerDiscrepancyResponse, CallTransferDiscrepancyResponse, ESRPDiscrepancyResponse, GISDiscrepancyResponse, IMRDiscrepancyResponse, LISDiscrepancyResponse, LoggingDiscrepancyResponse, PSAPDiscrepancyResponse, MCSDiscrepancyResponse, NetworkDiscrepancyResponse, OriginatingServiceDiscrepancyResponse, PermissionsDiscrepancyResponse, PolicyDiscrepancyResponse, PolicyStoreDiscrepancyResponse, SIPDiscrepancyResponse	This document
NoError	Validation Response	PolicyDiscrepancyResponse	This document
NoSuchLocation	Validation Response	LoSTDiscrepancyResponse	This document
NoSuchPolicy	Validation Response	PolicyStoreDiscrepancyResponse	This document
OmittedField	Problem	GISDiscrepancyReport	This document
OPTIONS	Problem	SIPDiscrepancyReport	This document
OtherADR	Problem	ADRDiscrepancyReport	This document
OtherBCF	Problem	BCFDiscrepancyReport	This document
OtherConflict	Problem	PolicyDiscrepancyReport	This document
OtherGIS	Problem	GISDiscrepancyReport	This document
OtherIMR	Problem	IMRDiscrepancyReport	This document
OtherLIS	Problem	LISDiscrepancyReport	This document
OtherLogging	Problem	LoggingDiscrepancyReport	This document
OtherLost	Problem	LoSTDiscrepancyResport	This document
OtherOSP	Problem	OriginatingServiceDiscrepancyReport	This document
OtherPermissions	Problem	PermissionsDiscrepancyReport	This document

© Copyright 2011-2022 National Emergency Number Association, Inc.

Token	Name	DiscrepancyReports	Reference
OtherResponse	Validation Response	ADRDiscrepancyResponse, BCFDiscrepancyReport, CallTakerDiscrepancyResponse, CallTransferDiscrepancyResponse, ESRPDiscrepancyResponse, GISDiscrepancyResponse, IMRDiscrepancyResponse, LISDiscrepancyResponse, LoggingDiscrepancyResponse, LoSTDiscrepancyReport, LoSTDiscrepancyResponse, MCSDiscrepancyResponse, NetworkDiscrepancyResponse, OriginatingServiceDiscrepancyResponse, PermissionsDiscrepancyResponse, PolicyDiscrepancyResponse, PolicyStoreDiscrepancyResponse, SIPDiscrepancyResponse	This document
OtherLVF	Problem	LoSTDiscrepancyReport	This document
OtherNetwork	Problem	NetworkDiscrepancyReport	This document
OtherPolicy	Problem	PolicyDiscrepancyReport	This document
Overlap	Problem	GISDiscrepancyReport	This document
OwnLocationUnavailable	Problem	LISDiscrepancyReport	This document
PacketLatency	Problem	NetworkDiscrepancyReport	This document
PacketLoss	Problem	NetworkDiscrepancyReport	This document
PermissionsCorrected	Validation Response	LISDiscrepancyResponse	This document
PerPolicy	Validation Response	BCFDiscrepancyReport, ESRPDiscrepancyResponse, LISDiscrepancyResponse, PermissionsDiscrepancyResponse	This document
PIDFLOtoMSAG	ServiceCall	MCSDiscrepancyReport	This document
Policy	Validation Response	ESRPDiscrepancyResponse	This document

© Copyright 2011-2022 National Emergency Number Association, Inc.

Token	Name	DiscrepancyReports	Reference
PolicyAdded	Validation Response	PolicyStoreDiscrepancyResponse	This document
PolicyAltered	Problem	PolicyStoreDiscrepancyReport	This document
PolicyCorrected	Validation Response	PolicyDiscrepancyResponse	This document
PolicyInvalid	Problem	PolicyStoreDiscrepancyReport	This document
PolicyMissing	Problem	PolicyStoreDiscrepancyReport	This document
PolicyUpdated	Validation Response	PolicyStoreDiscrepancyResponse	This document
ProblemCorrected	Validation Response	ADRDiscrepancyResponse, CallTransferDiscrepancyResponse, ESRPDiscrepancyResponse, IMRDiscrepancyResponse, MCSDiscrepancyResponse, NetworkDiscrepancyResponse, OriginatingServiceDiscrepancyResponse	This document
QoS	Problem	BCFDiscrepancyReport	This document
QueryTimeOut	Problem	OriginatingServiceDiscrepancyReport	This document
ReceivedIncorrectData	Problem	ADRDiscrepancyReport	This document
RecordsCorrected	Validation Response	LISDiscrepancyResponse	This document
ReferenceNotResolved	Problem	ADRDiscrepancyReport	This document
RequiredMedia	Problem	PSAPDiscrepancyReport	This document
ResponseConfusing	Problem	IMRDiscrepancyReport	This document
ResponseIncorrect	Problem	IMRDiscrepancyReport	This document
RetrieveLogEventError	Problem	LoggingDiscrepancyReport	This document
RouteIncorrect	Problem	LoSTDiscrepancyReport	This document
Routing	Problem	NetworkDiscrepancyReport	This document
ScriptLogicFailure	Problem	IMRDiscrepancyReport	This document
ServiceBoundaryIncorrect	Problem	LoSTDiscrepancyReport	This document
ServiceNumberIncorrect	Problem	LoSTDiscrepancyReport	This document
Severe	Severity	DiscrepancyReportRequest	This document
Signaling	Problem	SIPDiscrepancyReport	This document

© Copyright 2011-2022 National Emergency Number Association, Inc.

Token	Name	DiscrepancyReports	Reference
SignatureVerificationFailure	Problem	PolicyStoreDiscrepancyReport	This document
STIerror	Problem	OriginatingServiceDiscrepancyReport	This document
TimeoutDHCP	Problem	NetworkDiscrepancyReport	This document
TimeoutDNS	Problem	NetworkDiscrepancyReport	This document
TooManyURIs	Problem	ADRDiscrepancyReport	This document
TrafficNotBlocked	Problem	BCFDiscrepancyReport	This document
TrafficNotBlockedBadActor	Problem	BCFDiscrepancyReport	This document
TransferCorrect	ValidationResponse	CallTakerDiscrepancyResponse	This document
TRUE	LocationCorrect	ESRPDiscrepancyReport, OriginatingServiceDiscrepancyReport	This document
TTY	Problem	BCFDiscrepancyReport	This document
UnableAuthenticate	Problem	PermissionsDiscrepancyReport	This document
UnableDelete	Problem	PermissionsDiscrepancyReport	This document
UnableRead	Problem	PermissionsDiscrepancyReport	This document
UnableSubscribe	Problem	PermissionsDiscrepancyReport	This document
UnableWrite	Problem	PermissionsDiscrepancyReport	This document
Unknown	LocationCorrect	ESRPDiscrepancyReport, OriginatingServiceDiscrepancyReport	This document
UnknownBlock	Problem	ADRDiscrepancyReport	This document
UnknownPSAP	Problem	PolicyDiscrepancyReport	This document
UnknownScript	Problem	IMRDiscrepancyReport	This document
VerificationFailure	Problem	PolicyDiscrepancyReport	This document

10.35 "Event Package" Registry

IANA is requested to add the following entries to the Event Package registry:

Name	Reference
ElementState	This document
ServiceState	This document
QueueState	This document
ESRPNotify	This document
AbandonedCall	This document
GapOverlap	This document

© Copyright 2011-2022 National Emergency Number Association, Inc.

10.36 "Agent States" Registry

IANA is requested to add the following entries to the AgentStates registry:

State	Description	Reference
LoggedOut	Not currently logged in to the queue	This document
Break	Not at the console and unavailable to take a call	This document
Waiting	Not engaged	This document
Active	On a call	This document
Hold	On a call, have the call on hold	This document
Reserved	Temporarily aleryted to receive a specific call, not ready to take another. Will transition to Active when call is answered.	This document

11 Impacts, Considerations, Abbreviations, Terms, and Definitions

11.1 Operations Impacts Summary

This standard will have a profound impact on the operation of 9-1-1 services and PSAPs. New data formats, more rigid data structure requirements, new functions, new databases, new call sources, new media types, new security challenges, and more, will impact the operation of 9-1-1 systems, PSAPs, their contractors, and access and originating networks.

Nevertheless, the basic function, and the fundamental processes used to process calls, will not change substantially. NENA Committees are working diligently to provide appropriate procedures to match this specification.

11.2 Technical Impacts Summary

This standard supports end-to-end IP connectivity; gateways are used to accommodate legacy wireline and wireless originating networks that are non-IP as well as legacy Public Safety Answering Points (PSAPs) that interconnect to the i3 solution architecture, as described herein. NENA i3 introduces the concept of an Emergency Services IP network (ESInet), which is designed as an IP-based inter-network (network of networks) that can be shared by all public safety agencies that may be involved in any emergency, and a set of core services that process 9-1-1 calls on that network (NGCS – NG9-1-1 Core Services). The i3 Public Safety Answering Point (PSAP) is capable of receiving IP-based signaling and media for delivery of emergency calls conformant to the i3 standard.

Getting to the i3 solution from the current E9-1-1 infrastructure implies a transition from existing legacy originating network and 9-1-1 PSAP interconnections to next generation

© Copyright 2011-2022 National Emergency Number Association, Inc.

interconnections. This document describes how NG9-1-1 works after transition, including ongoing interworking requirements for IP-based and TDM-based PSAPs and originating networks. It does not provide solutions for how PSAPs, originating networks, SRs, and ALI systems evolve. Rather, it describes the end point at which conversion is complete. At that point, SRs and existing ALI systems are decommissioned and all 9-1-1 calls are routed by the Emergency Call Routing Function (ECRF) and arrive at the ESInet/NGCS via SIP. This document supports both IP-based and legacy TDM-based systems.

TDM-based PSAPs are connected to the ESInet/NGCS via a gateway (the Legacy PSAP Gateway). The definition of the Legacy PSAP Gateway is broad enough so this type of gateway may serve both primary and secondary PSAPs that have not been upgraded.

Similarly, the scope includes gateways for legacy wireline and wireless originating networks (the Legacy Network Gateway) used by originating networks which cannot yet create call signaling matching the interfaces described in this document for the ESInet. It is not envisioned that legacy originating networks will evolve to IP interconnect in all cases, and thus the Legacy Network Gateways will be needed for the foreseeable future. This document considers all wireline, wireless, and other types of networks with IP interfaces, including IMS [49] networks, although the document only describes the external interfaces to the ESInet/NGCS, which a conforming network must support. This document describes a common interface to the ESInet/NGCS, to be used by all types of originating networks or devices. How originating networks, or devices within them, conform is not visible to the ESInet/NGCS and is out of scope. The interface conforms to the best practice described in IETF RFC 6881 [46]. ATIS 0700015 [151], which is based on 3GPP TS 24.229 [226] and TS 23.167 [49], describes how IMS originating networks deliver calls to the ESInet NGCS as defined in this document.

11.3 Security Impacts Summary

This document introduces many new security mechanisms that will impact network and PSAP operations. The most significant changes to current practices are:

- All transactions must be protected with authentication, authorization, integrity protection, and privacy mechanisms specified by this document;
- Common authentication (single sign-on) and common rights management/authorization functions are used for ALL elements in the network;
- Of necessity, PSAPs will be connected, indirectly through the ESInet, to the global Internet to accept calls. This means that PSAPs will likely experience deliberate attacks on their systems. The types of vulnerabilities that NG9-1-1 systems must manage and protect against will fundamentally change and will require constant vigilance to create a secure and reliable operating environment. NG9-1-1 systems must have robust detection and mitigation mechanisms to deal with such attacks.

© Copyright 2011-2022 National Emergency Number Association, Inc.

11.4 Recommendation for Additional Development Work

This is the second revision of this document. There are several sections in which it is noted that further work is needed, and future revisions will cover topics in more depth. The authoring committee chose to describe future work within the document, rather than maintain a separate document with future work. Where this version states that future work is needed, vendors may need to implement the function in a way that may not yet be interoperable with other implementations, and when the work is complete (in a future version of this document), changes in such implementations may be necessary. The following table lists sections in this document that refer to possible future work.

Section	Reference to future work
<various>	There are several references to "near real-time" in this document. Definitions, maximums, and/or implementation guidance is necessary for each instance of the term
2.5	An equivalent definition for Canadian addresses will be referenced in a future version of this document.
2.7	The effect on emergency calls already in progress when mitigation is enabled will be addressed in a future version of this document.
2.11	A future version of this document will standardize SNMP MIBs for each FE.
3.1.10	There is considerable flux in standardized Instant Messaging protocols. It is anticipated that there may be additional IM protocols supported by NG9-1-1 in the future, specifically XMPP. If such protocols are adopted, a future version of this document will describe the ESInet interface.
3.6	A standard NENA schema for WFS as used in the i3 SI layer replication protocol will be provided in a future version of this document.
3.7.14	A Discrepancy Report by an OSP toward the OCIF reporting an identity verification failure for a call from the OCIF will be addressed in a future edition of this document.
4.2.1.6	A future version of this document will describe how to include the condition values that triggered the notify in the body of the NOTIFY.
4.2.2.5	Using the latest data may be problematic in some situations. Making the rules for merging objects more explicit would limit cases of conflicting information. This will be covered in a future version of this document.

© Copyright 2011-2022 National Emergency Number Association, Inc.

Section	Reference to future work
4.2.3	Specific policy document structures will be specified for each of the policy instances defined for the ESRP in a future version of this document.
4.3.3.4	Service to access Additional Data for a location: Additional Data is associated with a site/structure. This will be addressed in a future version of this document.
4.6.1	Handling of media other than voice-only callbacks is incompletely specified and will be addressed in a future version of this document.
4.7.6	An ad hoc transfer call flow involving MSRP may be provided in a future version of this document.
4.8.1	Work is currently ongoing in the Internet Engineering Task Force (IETF) to define RTT mixing and a future version of this document will specify appropriate standards.
4.11.1	A privacy issue was identified associated with this mechanism. Since it will require substantive changes, this will be addressed in a future version of this document.
4.13.3	A future version of this document will describe how policies can restrict retrieval by more fine-grained criteria, for example allowing only agencies participating in a multi-agency incident to retrieve LogEvents about that incident.
4.12.3.7	In the EventTypes described below, there is a very large amount of logging including cases in which information is logged at both the sender and receiver. Future versions of this document will describe a way to control what must be logged, whether digital signatures will be deployed, and their mechanism for deployment.
4.12.3.7	A description of which elements generate which LogEvent types will be described in a future version of this document.
4.12.3.7	Mechanisms to support blind and supervised transfer are not defined in this document and will be standardized in a future version of this document. Logging of such transfers is still required.
4.15.3	A future version of this document will specify a more general way to connect the Service/Agency Locator Search Services.
4.21	The use of the CVT FE in the processing of 9-1-1 calls is for future study.

© Copyright 2011-2022 National Emergency Number Association, Inc.

Section	Reference to future work
4.21	The concept of Secure Telephone Identity is nascent. As such, it is expected that the referenced standards will evolve. A future version of this document will ensure alignment with the evolution of these standards, when appropriate.
4.22	A detailed description of IDX functionality/interfaces will be part of a future version of this document
5.2	The PCA CP/CPS MUST be in conformance with minimum standards to be provided in a future version of this document.
5.3	Specific definitions of the roles enumerated in this section will be defined in an informational document (NENA-INF) to be referenced in a future version of this document.
5.6	Occasionally data becomes orphaned and must come under new ownership to provide updates. A mechanism to re-home orphaned data will be provided in a future version of this document.
7	Specification for the conveyance of EIDOs between agencies, systems, and applications will appear in a future version of this document.
9	PSAP Management interface will be provided in a future version of this document.
Appendix A	A future version of this document will further clarify how conversion between legacy formats and NG9-1-1 formats is accomplished.

11.5 Anticipated Timeline

As this is a major change to the 9-1-1 system, adoption of this standard will take several years and is also dependent on the pace of change and evolution of originating network providers, access network providers, and PSAPs. Experience with the immediately prior major change to 9-1-1 (i.e., Phase II wireless) suggests that unless consensus among government agencies at the local, state, and federal levels, as well as network operators, vendors, and other service providers is reached, implementation for the majority of PSAPs could take a decade. The i3 Architecture Working Group chose technology commensurate with a 2- to 5-year implementation schedule.

11.6 Cost Factors

This is an all-new 9-1-1 system; the cost of everything will change. At this time, it is difficult to predict the costs of the system and more work will be needed by vendors and service providers to determine the impact of the changes on their products and operations. If implemented at a regional (multi-county) or state level, the cost of the new system may

© Copyright 2011-2022 National Emergency Number Association, Inc.

be significantly less, although in the transition from the existing system to the new one, duplicate elements and services may have to be maintained at a higher overall cost. The case may also be that costs are not reduced, but the improved service to the public justifies these costs. Note that the charge to the i3 Architecture Working Group was to NOT make costs a primary consideration in making technical decisions. Nevertheless, due to the pragmatic experience of the participants, the document tended to consider cost as one of the variables in making choices. Estimating the cost to deploy the entire NG9-1-1 system is the purview of other groups within and outside NENA.

11.7 Cost Recovery Considerations

Traditionally, much of the cost of the existing E9-1-1 Service Provider infrastructure has been supported through the collection of fees and surcharges on wireline and wireless telephone service. Changes in the telecommunications industry have caused the basis upon which the fees and surcharges are collected to be modified, and the architecture described in this document further sunders the assumptions on which the current revenue streams are based. It should be noted that the costs associated with operating the 9-1-1 environment envisioned within this document are no longer accurately predicted by the number of originating network subscribers residing in a given service area. This document does not make recommendations on how funding should be changed. See the NG Partner Program Funding Policy paper [105] for more on this subject.

11.8 Additional Impacts (non-cost related)

This effort is a part of the overall Next Generation 9-1-1 project. There are far-reaching impacts to the entire 9-1-1 system and public safety policies engendered by the changes in networks, databases, devices, interfaces, and mechanisms this document describes. See the NG Partner Program Policy Guidelines documents for more on these areas [106]. It is expected that originating networks will ultimately evolve, but i3 assumes this evolution to take place over time and in stages by use of supporting gateways to allow existing interfaces from originating networks to be supported until such time as the originating network provider is ready to migrate to IP. Nearly all systems in a PSAP must (eventually) evolve. All databases change, some are eliminated, some new ones created, others are modified. New relationships between agencies must be established, for example, to facilitate answering of calls out of area.

Some of the more significant impacts are the methods and procedures to migrate the current 9-1-1 system to Next Generation 9-1-1. The NG9-1-1 Transition Planning Committee is developing documents that describe the transition. This document only describes external interfaces to a PSAP. The internal PSAP subsystems and the

© Copyright 2011-2022 National Emergency Number Association, Inc.

interconnection between those subsystems must change. This is the responsibility of the NENA NG9-1-1 PSAP Systems Working Group.

11.9 Abbreviations, Terms, and Definitions

See NENA Master Glossary of 9-1-1 Terminology, NENA-ADM-000 [1], for a complete listing of terms used in NENA documents. All abbreviations used in this document are listed below, along with any new or updated terms and definitions.

Term or Abbreviation (Expansion)	Definition / Description
3GPP (3RD Generation Partner Project)	A collaboration agreement that was established in December 1998. The collaboration agreement brings together a number of telecommunications standards bodies which are known as "Organizational Partners".
3GPP2 (3rd Generation Partnership Project 2)	A collaborative third generation (3G) telecommunications specifications-setting project comprising North American and Asian interests developing global specifications for ANSI/TIA/EIA-41 Cellular Radio telecommunication Intersystem Operations network evolution to 3G and global specifications for the radio transmission technologies (RTTs) supported by ANSI/TIA/EIA-41. A sister project to 3GPP.
AACN (Advanced Automatic Crash Notification	An emergency call placed by a vehicle, initiated either automatically or manually, conveying telematics data. Also called a "telematics call".
ACK (Acknowledgement)	A message to indicate the receipt of data.
ACM (Address Complete Message)	An ISDN (Integrated Services Digital Network) User Part (ISUP) message returned from the terminating switch when the subscriber is reached and the phone starts ringing, or when the call traverses an interworking point and the intermediate trunk is seized.
Additional Data	Further information intended to be useful to a call taker or responder (e.g., about how the call was placed, the person(s) associated with the device placing the call, the location of the call, vehicle sensor data, medical device data, etc.)

© Copyright 2011-2022 National Emergency Number Association, Inc.

Term or Abbreviation (Expansion)	Definition / Description
ADR (Additional Data Repository)	A data retrieval facility for Additional Data. The ADR dereferences a URI passed in a Call-Info header field or PIDF-LO <provided-by> and returns an Additional Data object block. An Identity-Searchable Additional Data Repository (IS-ADR) returns Additional Data associated with an identity.
AES (Advanced Encryption Standard)	A Federal Information Processing Standard (FIPS)-approved cryptographic algorithm that is used to protect electronic data.
Agency	In NG9-1-1, an organization that is connected directly or indirectly to the ESInet. Public safety agencies are examples of Agency. An entity such as a company that provides a service in the ESInet can be an Agency. Agencies have identifiers and credentials that allow them access to services and data.
Agent	In NG9-1-1, an Agent is an authorized person – employee, contractor, or volunteer – who has one or more roles in an Agency. An Agent can also be an automaton in some circumstances (e.g., an IMR answering a call).
AIP (Access Infrastructure Provider)	The entity providing physical communications access to the subscriber. This access may be provided over telco wire, CATV cable, wireless, or other media. Usually, this term is applied to purveyors of broadband internet access but is not exclusive to them.
ALRS (Agency Locator Record Store)	A web service that, when presented with an agency locator URI, returns the agency locator record.
AMR (Adaptive Multi-Rate (codec))	An audio compression format optimized for speech coding that automatically changes coding rates in response to the input audio stream. Refer to RFC 4867.
AMR-WB (Adaptive Multi Rate (codec) – Wide Band)	An audio compression format optimized for wideband speech coding that automatically changes coding rates in response to the input audio stream. Refer to RFC 4867.
ANI (Automatic Number Identification)	Telephone number associated with the access line from which a call originates.

© Copyright 2011-2022 National Emergency Number Association, Inc.

Term or Abbreviation (Expansion)	Definition / Description
ANSI (American National Standards Institute)	Entity that coordinates the development and use of voluntary consensus standards in the United States and represents the needs and views of U.S. stakeholders in standardization forums around the globe. www.ansi.org
APCO (Association of Public Safety Communications Officials)	APCO is the world's oldest and largest not-for-profit professional organization dedicated to the enhancement of public safety communications. http://www.apcointl.org/
ATIS (Alliance for Telecommunications Industry Solutions)	A U.S.-based organization that is committed to rapidly developing and promoting technical and operational standards for the communications and related information technologies industry worldwide using a pragmatic, flexible, and open approach. www.atis.org
Authoritative	Definitive, master. Information has an authoritative source, normally the owner of the information or its designee. There is only one authoritative source. A specific element or service may be authoritative for a given implementation or jurisdiction.
B2BUA (Back-to-Back User Agent)	A SIP element that relays signaling mechanisms while performing some alteration or modification of the messages that would otherwise not be permitted by a proxy server. A logical entity that receives a request and processes it as a UAS (User Agent Server). In order to determine how the request should be answered, it acts as a UAC (User Agent Client) and generates requests. Unlike a proxy server it maintains dialog state and must participate in all requests sent on the dialogs it established.
BCF (Border Control Function)	Provides a secure entry into the ESInet for emergency calls presented to the network. The BCF incorporates firewall admission control, and may include anchoring of session and media as well as other security mechanisms to prevent deliberate or malicious attacks on PSAPs or other entities connected to the ESInet.
BISACS (Building Information Services And Control System)	A computer-based system that allows access to building information such as its structural layout and/or to monitor a particular building or set of buildings for alerts.

© Copyright 2011-2022 National Emergency Number Association, Inc.

Term or Abbreviation (Expansion)	Definition / Description
CAMA (Centralized Automatic Message Accounting)	A type of in-band analog transmission protocol that transmits telephone number via multi-frequency encoding. Originally designed for billing purposes.
CAP (Common Alerting Protocol)	A general format for exchanging emergency alerts, primarily designed as an interoperability standard for use among warning systems and other emergency information systems. Refer to http://docs.oasis-open.org/emergency/cap/
CDR (Call Detail Record)	A record stored in a database recording the details of a received or transmitted call (from NENA-STA-010). The data information sent to the ALI computer by a remote identifying device (PBX, Call Position Identifier, etc)
cid (Content Identifier [Content-ID])	A unique identifier assigned to a body part that allows the body part to be referenced in a SIP header field.
codec (COder/DECoder)	A standardized means for encoding and decoding media, especially audio and video.
CoS (Class of Service)	A designation in E9-1-1 that defines the service category of the telephony service. Examples are residential, business, Centrex, coin, PBX, VoIP, and wireless Phase II (WPH2).
CPE (Customer Premises Equipment)	Communications or terminal equipment located in the customer's facilities – Terminal equipment at a PSAP.
CSRC (Contributing Source)	As specified in RFC 3550, a source of a stream of RTP packets that has contributed to the combined stream produced by an RTP mixer.
Dereference	The act of exchanging a reference to an item by its value. For example, the dereference operation for location uses a protocol such as SIP or HELD to obtain a location value (PIDF-LO).
DES (Data Encryption Standard)	The data encryption standard (DES) is a common standard for data encryption and a form of secret key cryptography (SKC), which uses only one key for encryption and decryption. Public key cryptography (PKC) uses two keys, (i.e., one for encryption and one for decryption).
DHCP (Dynamic Host Control Protocol (i2); Dynamic Host Configuration Protocol)	A widely used configuration protocol that allows a host to acquire configuration information from a visited network and, in particular, an IP address.

© Copyright 2011-2022 National Emergency Number Association, Inc.

Term or Abbreviation (Expansion)	Definition / Description
DNS (Domain Name Server)	Used in the Internet today to resolve domain names. The input to a DNS is a domain name (e.g., telcordia.com); the response is the IP address of the domain. The DNS allows people to use easy to remember text-based addresses and the DNS translates those names into routable IP addresses.
DNS (Domain Name System)	A globally distributed database for the resolution of host names to numeric IP addresses.
DoS (Denial of Service)	A type of cyber-attack intended to overwhelm the resources of the target and deny the ability of legitimate users of the target the normal service the target provides. DDoS (Distributed Denial of Service Attack) A cyber-attack where the source is more than one, often thousands of, unique IP addresses. A DDoS attack occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. Such an attack is often the result of multiple compromised systems (for example a botnet) flooding the targeted system with traffic. TDoS (Telephone Denial of Service) Illegal attacks targeting the telephone network by generating numerous 9-1-1 phone calls, tying up the network and preventing an agency from receiving legitimate calls.
DSCP (Differentiated Services Code Point)	A means of classifying and managing network traffic and of providing quality of service (QoS) in modern Layer 3 IP networks. It uses the 6-bit Differentiated Services (DS) field in the IP header for the purpose of packet classification.
DSig (Digital Signature)	The XML syntax used to associate the cryptographic signature value with Web resources using XML markup.
DSL (Digital Subscriber Line)	A "last mile" solution that uses existing telephony infrastructure to deliver high speed broadband access. DSL standards are administered by the DSL Forum http://dslforum.org/.
DTLS (Datagram Transport Layer Security)	A communications protocol that provides security for datagram-based applications by allowing them to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery.

© Copyright 2011-2022 National Emergency Number Association, Inc.

Term or Abbreviation (Expansion)	Definition / Description
E9-1-1 (Enhanced 9-1-1)	A telephone system which includes network switching, database, and Public Safety Answering Point premise elements capable of providing automatic location identification data, selective routing, selective transfer, fixed transfer, and a call back number. The term also includes any enhanced 9-1-1 service so designated by the Federal Communications Commission in its Report and Order in WC Docket Nos. 04-36 and 05-196, or any successor proceeding.
ECRF (Emergency Call Routing Function)	A functional element in an ESInet which is a LoST protocol server in which location information (either civic address or geo-coordinates) and a Service URN serve as input to a mapping function that returns a URI used to route an emergency call toward the appropriate PSAP for the caller's location or towards a responder agency. • External ECRF: An ECRF instance that resides outside of an ESInet instance. • Internal ECRF: An ECRF instance that resides within and is only accessible from an ESInet instance.
E-CSCF (Emergency Call Session Control Function)	The entity in the IMS core network that handles certain aspects of emergency sessions, e.g. routing of emergency requests to the correct emergency center or PSAP.
EDXL (Emergency Data eXchange Language)	A broad initiative to create an integrated framework for a wide range of emergency data exchange standards to support operations, logistics, planning, and finance.
EIDD (Emergency Incident Data Document)	A National Information Exchange Model (NIEM) conformant object that is used to share emergency incident information between and among authorized entities and systems.
EIDO (Emergency Incident Data Object)	A JSON-based object that is used to share emergency incident information between and among authorized entities and systems. NENA has adopted the JSON-based EIDO (Emergency Incident Data Object) for sharing incident information among authorized NG9-1-1 entities and systems.

© Copyright 2011-2022 National Emergency Number Association, Inc.

Term or Abbreviation (Expansion)	Definition / Description
ESInet (Emergency Services IP Network)	A managed IP network that is used for emergency services communications, and which can be shared by all public safety agencies. It provides the IP transport infrastructure upon which independent application platforms and core services can be deployed, including, but not restricted to, those necessary for providing NG9-1-1 services. ESInets may be constructed from a mix of dedicated and shared facilities. ESInets may be interconnected at local, regional, state, federal, national, and international levels to form an IP-based inter-network (network of networks). The term ESInet designates the network, not the services that ride on the network. See NG9-1-1 Core Services.
ESN (Emergency Service Number)	A 3-5 digit number that represents one or more ESZs. An ESN is defined as one of two types: Administrative ESN and Routing ESN.
ESRK (Emergency Services Routing Key)	A 10-digit North American Numbering Plan number that uniquely identifies a wireless emergency call, is used to route the call through the network, and used to retrieve the associated ALI data.
ESRP (Emergency Service Routing Proxy)	An i3 functional element which is a SIP proxy server that selects the next hop routing within the ESInet based on location and policy. There is an ESRP on the edge of the ESInet. There is usually an ESRP at the entrance to an NG9-1-1 PSAP. There may be one or more intermediate ESRPs between them. • Originating ESRP: The first routing element within the Next Generation Core Services (NGCS). It receives calls from the BCF at the edge of the ESInet. • Terminating ESRP: The last ESRP for a call in NGCS.
EVRC (Enhanced Variable Rate Codec) Narrowband	A speech codec developed to offer mobile carriers more network capacity while not increasing bandwidth requirements.
EVRC-WB (Enhanced Variable Rate Wideband Codec)	A speech codec providing enhanced (wideband) voice quality.

© Copyright 2011-2022 National Emergency Number Association, Inc.

Term or Abbreviation (Expansion)	Definition / Description
FAC (Facility [SS7 message])	A message sent in either direction at any phase of the call to request an action at another exchange.
FCC (Federal Communications Commission)	An independent U.S. government agency overseen by Congress, the Federal Communications Commission regulates interstate and international communications by radio, television, wire, satellite, and cable in all 50 states, the District of Columbia, and U.S. territories.
FCI (Feature Code Indicator)	Information sent in either direction to invoke a specific feature operation at the terminating or originating switch
FE (Functional Element) AKA: Functional Entity	A set of software features that may be combined with hardware interfaces and operations on those interfaces to accomplish a defined task.
FQDN (Fully Qualified Domain Name)	The complete domain name for a specific computer, or host, on the Internet.
g.711 a-law	An ITU-T Recommendation for an audio codec for telephony in non-North American regions.
g.711 mu-law	An ITU-T Recommendation for an audio codec for telephony in the North American region.
GCS (Geocode Service)	An NG9-1-1 service providing geocoding and reverse-geocoding.
GDP (Generic Digits Parameter)	Identifies the type of address to be presented in calls set up or additional numeric data relevant to supplementary services such as LNP or E9-1-1.
geopriv (Geographic Location/Privacy)	The name of an IETF work group, now dormant, which created location representation formats such as PIDF-LO and protocols for transporting them, such as HELD used in NG9-1-1. See https://datatracker.ietf.org/wg/geopriv/charter/
GeoRSS (Geodetic Really Simple Syndication)	A simple mechanism used to encode GML in RSS feeds for use with the ATOM protocol.
geoShape element (Geodetic Shape)	One of a list of shapes defined originally by the IETF and standardized by the Open Geospatial Consortium that can be found in a PIDF-LO. Includes point, circle, ellipse, arc band, polygon, and 3-D versions of same.

© Copyright 2011-2022 National Emergency Number Association, Inc.

Term or Abbreviation (Expansion)	Definition / Description
GIS (Geographic Information System)	A system for capturing, storing, displaying, analyzing, and managing data and associated attributes which are spatially referenced.
GML (Geography Markup Language)	An XML grammar for expressing geographical features standardized by the OGC.
GRUU (Globally Routable User agent URI)	A SIP URI which identifies a specific endpoint at which a user is signed on that is routable on the Internet.
H.264/MPEG-4	An ITU-T Recommendation and Motion Picture Expert Group standard for a video codec
HELD (HTTP-Enabled Location Delivery Protocol)	A protocol that can be used to acquire Location Information (LI) from a LIS within an access network as defined in IETF RFC 5985.
HTTP (HyperText Transfer Protocol)	Typically used between a web client and a web server that transports HTML and/or XML.
HTTPS (HyperText Transfer Protocol Secure)	HTTP with secure transport (Transport Layer Security or its predecessor, Secure Sockets Layer)
i3	"i3" refers to the NG9-1-1 system architecture defined by NENA, which standardizes the structure and design of Functional Elements making up the set of software services, databases, network elements and interfaces needed to process multi-media emergency calls and data for NG9-1-1. (See NG9-1-1 Core Services (NGCS), ESInet and NG9-1-1.)
IAM (Initial Address Message)	The first message sent in a call set-up by a Switch or Exchange to other partner exchange. Refer to http://www.wapopia.com/techfaq/gsm-faq/what-is-initial-address-message-iam/
IANA (Internet Assigned Numbers Authority)	The entity that oversees global IP address allocation; DNS root zone management, and other Internet protocol assignments. www.iana.org
ICE (Interactive Connectivity Establishment)	A mechanism for endpoints to establish RTP connectivity in the presence of NATs and other middle-boxes.

© Copyright 2011-2022 National Emergency Number Association, Inc.

Term or Abbreviation (Expansion)	Definition / Description
IDP (Identity Provider)	An entity which authenticates users and supplies services with a "token" that can be used in subsequent operations to refer to an authorized user.
IDX (Incident Data eXchange)	A Functional Element that facilitates the exchange of Emergency Incident Data Objects (EIDOs) among other Functional Elements both within and external to an agency.
IETF (Internet Engineering Task Force)	Lead standard-setting authority for Internet protocols.
IM (Instant Messaging)	A method of communication, generally using text, in which more than a character at a time is sent between parties nearly instantaneously.
IMR (Interactive Media Response)	An automated service used to play announcements, record responses, and interact with callers using any or all of audio, video, and text.
IMS (Internet Protocol Multimedia Subsystem)	The IP Multimedia Subsystem comprising all 3GPP/3GPP2 core network elements providing IP multimedia services that support audio, video, text, and pictures, alone or in combination, delivered over a packet-switched domain.
Incident Tracking Identifier	An identifier assigned by the first element in the first ESInet that handles an emergency call or declares an incident. Incident Tracking Identifiers are globally unique.
INVITE	A SIP transaction used to initiate a session (See re-INVITE).
IP (Internet Protocol)	The method by which data is sent from one computer to another on the Internet or other networks.
IPv4 (Internet Protocol version 4)	The fourth version of the Internet Protocol; uses 32-bit addresses.
IPv6 (Internet Protocol version 6)	The most recent version of the Internet Protocol; uses 128-bit addresses.
IS-ADR (Identity Searchable Additional Data Repository)	An Additional Data Repository providing a service that can search for Additional Data based on a sip/sips or tel URI: (e.g., Additional Data about the caller).
ISDN (Integrated Services Digital Network)	International standard for a public communication network to handle circuit-switched digital voice, circuit-switched data, and packet-switched data.

© Copyright 2011-2022 National Emergency Number Association, Inc.

Term or Abbreviation (Expansion)	Definition / Description
ISP (Internet Service Provider)	A company that provides Internet access to other companies and individuals.
ISUP (Integrated Services Digital Network User Part)	A message protocol to support call set up and release for interoffice voice call connections over SS7 Signaling.
ITU (International Telecommunication Union)	The telecommunications agency of the United Nations established to provide worldwide standard communications practices and procedures. Formerly CCITT.
KP (Key Pulse)	An MF signaling tone (digit).
LIF (Location Interwork Function)	The functional component of a Legacy Network Gateway which is responsible for taking the appropriate information from the incoming signaling (i.e., calling number/ANI, ESRK, cell site/sector) and using it to acquire location information that can be used to route the emergency call and to provide location information to the PSAP. In a Legacy PSAP Gateway, this functional component takes the information from an ALI query and uses it to obtain location from a LIS.
LIS (Location Information Server)	A functional element that provides locations of endpoints. A LIS can provide Location-by-Reference, or Location-by-Value, and, if the latter, in geodetic or civic forms. A LIS can be queried by an endpoint for its own location, or by another entity for the location of an endpoint. In either case, the LIS receives a unique identifier that represents the endpoint, for example an IP address, circuit-ID, or MAC address, and returns the location (value or reference) associated with that identifier. The LIS is also the entity that provides the dereferencing service, exchanging a location reference for a location value.
LNG (Legacy Network Gateway)	An NG9-1-1 Functional Element that provides an interface between a non-upgraded legacy originating network and a Next Generation Core Services (NGCS)-enabled network.

© Copyright 2011-2022 National Emergency Number Association, Inc.

Term or Abbreviation (Expansion)	Definition / Description
LO (Location Object)	In an emergency calling environment, the LO is used to refer to the current position of an endpoint that originates an emergency call. The LO is expected to be formatted as a Presence Information Data Format – Location Object (PIDF-LO) as defined by the IETF in RFC 4119, updated by RFCs 5139, 5491, and 7459, and extended by RFC 6848. The LO may be: • Geodetic – shape, latitude(s), longitude(s), elevation, uncertainty, confidence and the datum which identifies the coordinate system used. NENA prescribes that geodetic location information will be formatted using the World Geodetic System 1984 (WGS 84) datum; • Civic location – a set of elements describing detailed street address information. For NG9-1-1 in the U.S., the civic LO must conform to the NENA Next Generation 9-1-1 (NG9-1-1) United States Civic Location Data Exchange Format (CLDXF) Standard (NENA-STA-004); • or a combination thereof.
LogEvent	A standardized JSON object containing information about a processing event that is stored in and retrieved from the Logging Service.
LoST (Location to Service Translation) Protocol	A protocol that takes location information and a Service URN and returns a URI. Used generally for location-based call routing. In NG9-1-1, used as the protocol for the ECRF and LVF.
LPG (Legacy PSAP Gateway)	A signaling and media interconnection point between an ESInet and a legacy PSAP. It plays a role in the delivery of emergency calls that traverse an i3 ESInet to get to a legacy PSAP, as well as in the transfer and alternate routing of emergency calls between legacy PSAPs and NG9-1-1 PSAPs. The Legacy PSAP Gateway supports an IP (i.e., SIP) interface towards the ESInet on one side, and a traditional MF or Enhanced MF interface (comparable to the interface between a traditional Selective Router and a legacy PSAP) on the other.

© Copyright 2011-2022 National Emergency Number Association, Inc.

Term or Abbreviation (Expansion)	Definition / Description
LRF (Location Retrieval Function)	The IMS-associated functional entity that handles the retrieval of location information for the emergency caller including, when required, interim location information, initial location information, and updated location information. The LRF may interact with a separate RDF or contain an integrated RDF in order to obtain routing information for an emergency call.
LSRG (Legacy Selective Router Gateway)	Provides an interface between a 9-1-1 Selective Router and an ESInet, enabling calls to be routed and/or transferred between Legacy and NG networks. A tool for the transition process from Legacy 9-1-1 to NG9-1-1.
LVF (Location Validation Function)	A functional element in an NGCS that is a LoST protocol server where civic location information is validated against the authoritative GIS database information. A civic address is considered valid if it can be located within the database uniquely, is suitable to provide an accurate route for an emergency call and adequate and specific enough to direct responders to the right location.
MCS (MSAG Conversion Service)	A web service providing conversion between PIDF-LO and MSAG data.
MDN (Mobile Directory Number)	The telephone number dialed to reach a wireless telephone.
MDS (Mapping Data Service)	Provides a PSAP call taker with information showing the location of an out-of-area caller.
MF (Multi-Frequency)	A type of in-band signaling used on analog interoffice and 9-1-1 trunks.
MIB (Management Information Base)	An object used with the Simple Network Management Protocol to manage a specific device or function.
MIME (Multipurpose Internet Mail Extensions)	A specification for formatting non-ASCII messages so that they can be sent over the Internet.

© Copyright 2011-2022 National Emergency Number Association, Inc.

Term or Abbreviation (Expansion)	Definition / Description
MPC/GMLC (Mobile Positioning Center/ Gateway Mobile Location Center)	A Functional Entity that provides an interface between the wireless originating network and the Emergency Services Network. The MPC/GMLC retrieves, forwards, stores, and controls position data within the location services network. It interfaces with the location server (e.g. Position Determining Entity [PDE]) for initial and updated position determination. The MPC/GMLC restricts access to provide position information only while an emergency service call is active.
MSAG (Master Street Address Guide)	A database of street names and house number ranges within their associated communities defining Emergency Service Zones (ESZs) and their associated Emergency Service Numbers (ESNs) to enable proper routing of 9-1-1 calls.
MSC (Mobile Switching Center)	The wireless equivalent of a Central Office, which provides switching functions for wireless calls.
MSRP (Message Session Relay Protocol)	A standardized mechanism for exchanging instant messages using SIP where a server relays messages between user agents.
MTP (Message Transfer Part)	A layer of the SS7 protocol providing the routing and network interface capabilities to support call setup.
NANP (North American Numbering Plan)	An integrated telephone numbering plan serving 20 North American countries that share telephone numbers in the +1 country code. www.nationalnanpa.com
NAPT (Network Address and Port Translation)	A methodology of remapping one IP address and port into another by modifying network address information in Internet Protocol (IP) datagram packet header fields while they are in transit across a traffic routing device.
NAT (Network Address Translation)	Maps a single public address to one or many internal addresses and all network IP addresses on the connected computers are local and cannot be seen by the outside world.
NENA (National Emergency Number Association)	A not-for-profit corporation established in 1982 to further the goal of "One Nation-One Number." NENA is a networking source and promotes research, planning, and training. NENA strives to educate, set standards, and provide certification programs, legislative representation, and technical assistance for implementing and managing 9-1-1 systems. www.nena.org

© Copyright 2011-2022 National Emergency Number Association, Inc.

Term or Abbreviation (Expansion)	Definition / Description
NG9-1-1 (Next Generation 9-1-1)	"Next Generation 9-1-1 services" means a secure, IP-based, open-standards system comprised of hardware, software, data, and operational policies and procedures that (A) provides standardized interfaces from emergency call and message services to support emergency communications; (B) processes all types of emergency calls, including voice, text, data, and multimedia information; (C) acquires and integrates additional emergency call data useful to call routing and handling; (D) delivers the emergency calls, messages, and data to the appropriate public safety answering point and other appropriate emergency entities based on the location of the caller; (E) supports data, video, and other communications needs for coordinated incident response and management; and (F) interoperates with services and networks used by first responders to facilitate emergency response. REF: Agreed to by NENA, NASNA, iCERT, and the National 9-1-1 Office representatives on 01/12/2018.
NGCS (Next Generation 9-1-1 [NG9-1-1] Core Services)	The base set of services needed to process a 9-1-1 call on an ESInet. Includes the ESRP, ECRF, LVF, BCF, Bridge, Policy Store, Logging Services, and typical IP services such as DNS and DHCP. The term NG9-1-1 Core Services includes the services and not the network on which they operate. See Emergency Services IP Network
NIF (NG9-1-1 Specific Interwork Function)	The functional component of a Legacy Network Gateway or Legacy PSAP Gateway which provides NG9-1-1-specific processing of the call not provided by an off-the-shelf protocol interwork gateway.
NPD (Numbering Plan Digit)	A component of the traditional 8-digit 9-1-1 signaling protocol between the Enhanced 9-1-1 Control Office and the PSAP CPE. Identifies 1 of 4 possible area codes.
NRS (NENA Registry System)	The entity provided by NENA to manage registries. http://technet.nena.org/nrs/registry/_registries.xml

© Copyright 2011-2022 National Emergency Number Association, Inc.

Term or Abbreviation (Expansion)	Definition / Description
NTP (Network Time Protocol)	A networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks.
OASIS (Organization for the Advancement of Structured Information Standards)	An organization that promulgates standards for data interchange. www.oasis-open.org
OGC (Open Geospatial Consortium)	A standards development organization that promulgates standards for the global geospatial community. http://www.opengeospatial.org/
OLI (Originating Line Identification parameter)	A parameter that conveys class of service information about the originator of a call.
OSI (Open Systems Interconnection)	A 7-layer hierarchical reference model structure developed by the International Standards Organization for defining, specifying, and relating communications protocols; not a standard or a protocol. Layer Description • (7) Application: Provides interface with network users • (6) Presentation: Performs format and code conversion • (5) Session: Manages connections for application programs • (4) Transport: Ensures end-to-end delivery • (3) Network: Handles network addressing and routing • (2) Data Link: Performs local addressing and error detection • (1) Physical: Includes physical signaling and interfaces
P-A-I (P-Asserted-Identity)	A header field in a SIP message containing a URI that the originating network asserts is the correct identity of the caller.
PCA (PSAP Credentialing Agency)	The root authority designated to issue and revoke security credentials (in the form of an X.509 certificate) to authorized 9-1-1 agencies in an i3-compliant infrastructure.

© Copyright 2011-2022 National Emergency Number Association, Inc.

Term or Abbreviation (Expansion)	Definition / Description
P-DCS-OSPS (PacketCable-Distributed Call Signaling-Operator Services Position System)	The architecture designed to facilitate the exchange of trusted information between telephone service providers that conveys customer-specific information and expectations about the parties involved in the call.
PHB (Per Hop Behaviors)	The action a router takes for a packet marked with a specific code point in the Diffserv QoS mechanism in IP networks.
PIDF (Presence Information Data Format)	Specified in IETF RFC 3863; it provides a common presence data format for Presence protocols, and also defines a new media type. A presence protocol is a protocol for providing a presence service over the Internet or any IP network.
PIDF-LO (Presence Information Data Format – Location Object)	Provides a flexible and versatile means to represent location information in a SIP header field using an XML schema.
PIF (Protocol Interworking Function)	That functional component of a Legacy Network Gateway or Legacy PSAP Gateway that interworks legacy PSTN signaling such as ISUP or CAMA with SIP signaling.
PKI (Public Key Infrastructure)	A set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption.
PRF (Policy Routing Function)	That functional component of an Emergency Service Routing Proxy that determines the next hop in the SIP signaling path using a policy.

© Copyright 2011-2022 National Emergency Number Association, Inc.

Term or Abbreviation (Expansion)	Definition / Description
PSAP (Public Safety Answering Point)	An entity responsible for receiving 9-1-1 calls and processing those calls according to a specific operational policy. • Primary PSAP: A PSAP to which 9-1-1 calls are routed directly from the 9-1-1 Control Office. • Secondary PSAP: A PSAP to which 9-1-1 calls are transferred from a Primary PSAP. • Alternate PSAP: A PSAP designated to receive calls when the primary PSAP is unable to do so. • Consolidated PSAP: A facility where multiple Public Safety Agencies choose to operate as a single 9-1-1 entity. • Legacy PSAP: A PSAP that cannot process calls received via i3-defined call interfaces (IP-based calls) and still requires the use of CAMA or ISDN trunk technology for delivery of 9-1-1 emergency calls. • Serving PSAP: The PSAP to which a call would normally be routed. • NG9-1-1 PSAP: This term is used to denote a PSAP capable of processing calls and accessing data services as defined in NENA's i3 specification, NENA NENA-STA-010, and referred to therein as an "i3 PSAP".
PSP (Provisioning Service Provider)	The component in an ESInet functional element that implements the provider side of an SPML interface used for provisioning
PSTN (Public Switched Telephone Network)	The network of equipment, lines, and controls assembled to establish communication paths between calling and called parties in North America.
QoS (Quality of Service)	As related to data transmission, a measurement of latency, packet loss, and jitter.
RDF (Routing Determination Function)	The IMS-associated functional entity, which may be integrated in a Location Server (e.g. GMLC) or in an LRF, and provides the proper outgoing address to the E-CSCF for routing the emergency request towards a PSAP. It can interact with a location functional entity (e.g., GMLC) to manage ESQK allocation and management and deliver location information to the PSAP.

© Copyright 2011-2022 National Emergency Number Association, Inc.

Term or Abbreviation (Expansion)	Definition / Description
REFER/Replaces	Use of the SIP REFER method together with a Replaces header field as part of a transfer operation to indicate that a new leg is to be created that replaces an existing call leg.
re-INVITE	A SIP INVITE transaction within an established session used to change the parameters of a call or refresh a session. See INVITE.
REL (Release) message	An ISUP message sent in either direction to release the circuit.
Request-URI	That part of a SIP message that indicates where the call is being routed. SIP Proxy servers commonly change the Request ID ("retargeting") to route a call towards the intended recipient.
Resource Priority	A header field used on SIP calls to indicate priority that proxy servers give to specific calls. The Resource Priority header field does not indicate that a call is an emergency call (see Request-URI).
REST (Representational State Transfer)	An interface that transmits domain-specific data over HTTP without an additional messaging layer such as SOAP or session tracking via HTTP cookies.
RFC (Request for Comment)	A document published by the Internet Engineering Task Force (IETF). Note that the name is an historic artifact—An RFC is finalized. RFCs are never revised; updates are published as new RFCs. Errata are noted separately. (Documents for which input and comments are requested are called Internet Drafts. Most RFCs are originally published as an Internet Draft).
RLC (Release Complete)	An ISUP message sent to acknowledge the release (REL) message indicating that the circuit is idle afterward and can be used again.
ROH (Receiver Off-Hook)	A call state in which the recipient's hand set is not in the cradle.
ROHC (Robust Header Compression)	A standardized method to compress the IP, UDP, UDP-Lite, RTP, and TCP headers of Internet packets.

© Copyright 2011-2022 National Emergency Number Association, Inc.

Term or Abbreviation (Expansion)	Definition / Description
RTCP (Real-time Transport Control Protocol)	A sister protocol of RTP and provides out-of-band control information for an RTP flow. It partners RTP in the delivery and packaging of multimedia data, but does not transport any data itself. It is used periodically to transmit control packets to participants in a streaming multimedia session. The primary function of RTCP is to provide feedback on the quality of service being provided by RTP. It gathers statistics on a media connection and information such as bytes sent, packets sent, lost packets, jitter, feedback, and round trip delay. An application may use this information to increase the quality of service perhaps by limiting flow, or maybe using a low compression codec instead of a high compression codec. RTCP is used for Quality of Service (QoS) reporting.
RTP (Real-time Protocol)	An IP protocol used to transport media (voice, video, text) which has a real-time constraint.
RTSP (Real-time Streaming Protocol)	A network control protocol designed for use in entertainment and communications systems to control streaming media servers.
RTT (Real-time Text)	Text transmission that is one character at a time, as in TTY.
SAML (Security Assertion Markup Language)	An XML-based, open-standard data format for exchanging authentication and authorization data between an identity provider and another party.
SAP (Service Activation Parameter)	A parameter included in an SS7 call control message to invoke an action at another node or report the result of such an action.

© Copyright 2011-2022 National Emergency Number Association, Inc.

Term or Abbreviation (Expansion)	Definition / Description
SCTP (Stream Control Transport Protocol)	Defined by IETF RFC 4960 as the transport layer to carry signaling messages over IP networks. SCTP/T is just one of the many products in the Adax Protocol Software (APS) SIGTRAN suite that has been designed for Convergence, Wireless, and Intelligent Networks. Compliant with IETF RFC 4960 and RFC 3309, SCTP/T (SCTP for Telephony) is implemented in the OS kernel. SCTP/T provides a transport signaling framework for IP networks that enhances the speed and capability of SSCS/HSL and can be deployed over T1/E1, Ethernet, and ATM OC3 physical media interfaces. In addition to the services specified in IETF RFC 4960, Adax SCTP/T also provides a transport framework with levels of service quality and reliability as those expected from a Public Switched Telephone Network (PSTN).
SDO (Standards Development Organization)	An entity whose primary activities are developing, coordinating, promulgating, revising, amending, reissuing, interpreting, or otherwise maintaining standards that address the interests of a wide base of users outside the standards development organization.
SDP (Session Description Protocol)	A standard syntax contained in a signaling message to negotiate a real-time media session. See RFC 4566.
Security Posture	An event, part of Service State, which represents a downstream entity's current security state (Green for normal, Yellow for suspicious activity, Orange for fraudulent events, Red for under active attack).
Service URN (Uniform Resource Name)	A URN with "service" as the first component supplied as an input in a LoST request to an ECRF to indicate which service boundaries to consider when determining a response. A Request-URI with the service URN of "urn:service:sos" is used to mark a call as an emergency call. See Request-URI.
SHA (Secure Hash Algorithm)	One of a number of fixed-size, cryptographic algorithms promulgated by the National Institute of Standards and Technology used to provide integrity protection for messages, files, and other data objects.

© Copyright 2011-2022 National Emergency Number Association, Inc.

Term or Abbreviation (Expansion)	Definition / Description
SI (Spatial Interface)	A standardized interface between the GIS and the functional elements that consume GIS data, such as the ECRF/LVF, Map Database Services, etc.
SIO (Service Information Octet)	An eight-bit data field that is present in an SS7 message signal unit and is comprised of the service indicator and the sub-service field. It is used to determine the user part to which an incoming message should be delivered.
SIP (Session Initiation Protocol)	A protocol specified by the IETF (RFC 3261) that defines a method for establishing multimedia sessions over the Internet. Used as the call signaling protocol in VoIP, NENA i2, and NENA i3 .
SLA (Service Level Agreement)	A contract between a service provider (either internal or external) and the end user that defines the level of service expected from the service provider. SLAs are output-based in that their purpose is specifically to define what the customer will receive.
SMS (Short Message Service)	A service typically provided by mobile carriers that sends short (160 characters or fewer) messages to an endpoint. SMS is often fast, but is not real-time.
SNMP (Simple Network Management Protocol)	A protocol defined by the IETF used for managing devices on an IP network.
SOA (Service Oriented Architecture)	A model in computer software design in which application components provide a repeatable business activity to other components using a communications protocol, typically over a network.
SOAP (Simple Object Access Protocol)	A protocol for exchanging XML-based messages over a computer network, normally using HTTP. SOAP forms the foundation layer of the Web services stack, providing a basic messaging framework that more abstract layers can build upon.
SOS URN	A service URN starting with "urn:service:sos" which is used to mark calls as emergency calls as they traverse an IP network and to specify the desired emergency service in an ECRF request. See Service Uniform Resource Name.

© Copyright 2011-2022 National Emergency Number Association, Inc.

Term or Abbreviation (Expansion)	Definition / Description
SR (Selective Router) AKA: Enhanced 9-1-1 Control Office	The Central Office switch that provides the tandem switching of 9-1-1 calls. It controls delivery of the voice call with ANI to the PSAP and provides Selective Routing, Speed Calling, Selective Transfer, Fixed Transfer, and certain maintenance functions for each PSAP.
SR (Selective Routing)	The process by which 9-1-1 calls/messages are routed to the appropriate PSAP or other designated destination, based on the caller's location information, and may also be impacted by other factors, such as time of day, call type, etc. Location may be provided in the form of an MSAG-valid civic address or in the form of geodetic coordinates (longitude and latitude). Location may be conveyed to the system that performs the selective routing function in the form of ANI or pseudo-ANI associated with a pre-loaded ALI database record (in Legacy 9-1-1 systems), or in real-time in the form of a Presence Information Data Format-Location Object (PIDF-LO) (in NG9-1-1 systems) or whatever forms are developed as 9-1-1 continues to evolve.
SRTP (Secure Real-time Protocol)	An IP protocol used to securely transport media (voice, video, text) which have a real-time constraint.
SRV (Service)	A specification of data in the Domain Name System defining the location, (i.e. the hostname and port number) of servers for specified services.
SS7 (Signaling System 7)	An out-of-band signaling system used to provide basic routing information, call set-up, and other call termination functions. Signaling is removed from the voice channel itself and put on a separate data network.
SSRC (Synchronization Source)	As specified in RFC 3550, the source of a stream of RTP packets, identified by a 32-bit numeric SSRC identifier carried in the RTP header so as not to be dependent upon the network address.
STUN (Session Traversal Utilities for NAT)	A protocol that serves as a tool for other protocols in dealing with Network Address Translator (NAT) traversal

© Copyright 2011-2022 National Emergency Number Association, Inc.

Term or Abbreviation (Expansion)	Definition / Description
TCP (Transmission Control Protocol)	A communications protocol linking different computer platforms across networks. TCP/IP functions at the 3rd and 4th levels of the Open System Interconnection (OSI) model.
TDM (Time Division Multiplexing)	A digital multiplexing technique for combining a number of signals into a single transmission facility by interweaving pieces from each source into separate time slots.
TLS (Transport Layer Security)	An Internet protocol that operates between the IP layer and TCP and provides hop-by-hop authentication, integrity, protection, and privacy using a negotiated cipher-suite.
TN (Telephone Number)	A sequence of digits assigned to a device to facilitate communications via the public switched telephone network or other private network.
TRD (Technical Requirements Document)	NENA Technical Requirements Document, developed by a Technical Committee, is used as basis for a NENA Technical Committee or outside Standards Development Organization (SDO) to develop formal industry-accepted standards or guidelines.
TSP (Telematics Service Provider)	Companies which provide telematics (communications and data) services.
TTY (Teletypewriter) AKA TDD (Telecommunications Device for the Deaf)	The phrase TTY (or Teletype device) is how the deaf community used to refer to the extremely large machines they used to type messages back and forth over the phone lines. A TDD operates in a similar way, but is a much smaller desktop machine. The deaf community has used the phrase "TTY" and sometimes uses it interchangeably with "TDD." http://www.gallaudet.edu/about/history-and-traditions/tty-relays-and-closed-captions
TURN (Traversal Using Relays Around NAT)	A mechanism for establishing RTP connections through some kinds of NAT devices that won't allow two endpoints to connect directly. TURN uses a relay outside the NAT boundaries.
TYS (Type of Service)	A designation in E9-1-1 that specifies if caller's service is published or non-published and if it is a foreign exchange outside the E9-1-1 serving area.

© Copyright 2011-2022 National Emergency Number Association, Inc.

Term or Abbreviation (Expansion)	Definition / Description
UA (User Agent)	As defined for SIP in IETF RFC 3261[10], the User Agent represents an endpoint in the IP domain, a logical entity that can act as both a user agent client (UAC) that sends requests, and as user agent server (UAS) responding to requests.
UAC (User Agent Client)	Refer to IETF RFC 3261 for the following definition. "A user agent client is a logical entity that creates a new request, and then uses the client transaction state machinery to send it. The role of UAC lasts only for the duration of that transaction. In other words, if a piece of software initiates a request, it acts as a UAC for the duration of that transaction. If it receives a request later, it assumes the role of a user agent server for the processing of that transaction."
UAS (User Agent Server)	Refer to IETF RFC 3261 for the following definition. "A user agent server is a logical entity that generates a response to a SIP request. The response accepts, rejects, or redirects the request. This role lasts only for the duration of that transaction. In other words, if a piece of software responds to a request, it acts as a UAS for the duration of that transaction. If it generates a request later, it assumes the role of a user agent client for the processing of that transaction."
UDDI (Universal Description, Discovery and Integration)	An XML-based registry for businesses worldwide, which enables businesses to list themselves and their services on the Internet.
UDP (User Datagram Protocol)	One of several core protocols commonly used on the Internet. Used by programs on networked computers to send short messages, called datagrams, between one another. UDP is a lightweight message protocol compared to TCP, is stateless, and more efficient at handling lots of short messages from many clients.

© Copyright 2011-2022 National Emergency Number Association, Inc.

Term or Abbreviation (Expansion)	Definition / Description
URI (Uniform Resource Identifier)	An identifier consisting of a sequence of characters matching the syntax rule that is named <URI> in RFC 3986. It enables uniform identification of resources via a set of naming schemes. A URI can be further classified as a lo A URI is an identifier consisting of a sequence of characters matching the syntax rule that is named <URI> in RFC 3986. It enables uniform identification of resources via a set of naming schemes. A URI can be further classified as a locator, a name, or both. The term "Uniform Resource Locator" (URL) refers to the subset of URIs that, in addition to identifying a resource, provides a means of locating the resource by describing its primary access mechanism (e.g., its network "location").cator, a name, or both. The term "Uniform Resource Locator" (URL) refers to the subset of URIs that, in addition to identifying a resource, provides a means of locating the resource by describing its primary access mechanism (e.g., its network "location"). The term "Uniform Resource Name" (URN) has been used historically to refer to both URIs under the "urn" scheme [RFC2141], which are required to remain globally unique and persistent even when the resource ceases to exist or becomes unavailable, and to any other URI with the properties of a name. An example of a URI that is neither a URL nor a URN is sip:psap@example.com
URL (Uniform Resource Locator)	A type of URI specifically used for describing and navigating to a resource (e.g., http://www.nena.org)
URN (Uniform Resource Name)	A type of URI. Uniform Resource Names (URNs) are intended to serve as persistent, location-independent resource identifiers and are designed to make it easy to map other namespaces (which share the properties of URNs) into URN-space. An example of a URN is urn:service:sos. RFC 2141.
US-CERT (United States Computer Emergency Readiness Team)	Part of the Department of Homeland Security's (DHS) National Cybersecurity and Communications Integration Center (NCCIC), the US-CERT leads efforts to improve the Nation's cybersecurity posture, coordinate cyber information sharing, and proactively manage cyber risks to the Nation.

© Copyright 2011-2022 National Emergency Number Association, Inc.

Term or Abbreviation (Expansion)	Definition / Description
USPS (United States Postal Service)	An independent agency of the United States government responsible for providing mail service in the United States.
UTC (Universal Coordinated Time)	The primary time standard in the world based on the time zone in Greenwich, England. Also known as Zulu or Greenwich Mean Time (GMT). Time provided by National Institute of Standards and Technology (NIST) and United States Naval Observatory (USNO).
VEDS (Vehicle Emergency Data Sets)	A uniform data set for the transmission of Advanced Automatic Collision Notification (AACN) data by automobiles and automotive Telematics Service Providers (TSPs).
VESA (Valid Emergency Services Authority)	This organization is the root source of all certificates. It is responsible for identifying and issuing certificates either directly to end-using entities or through delegate credential authorities. It is responsible for ensuring that any delegate credential authority that it identifies is properly qualified and operating with sufficient security and legitimacy to perform this role. Where VESA issues certificates directly to end users, it also has the responsibilities of a delegate credential authority in those cases.
VoIP (Voice over Internet Protocol)	Technology that permits delivery of voice calls and other real-time multimedia sessions over IP networks.
VPN (Virtual Private Network)	A network implemented on top of another network, and private from it, providing transparent services between networks or devices and networks. VPNs often use some form of cryptographic security to provide this separation.
VSP (VoIP Service Provider)	A company that offers VoIP telecommunications services that may be used to generate a 9-1-1 call, and interconnects with the 9-1-1 network.
WFS (Web Feature Service)	A web service that allows a client to retrieve and update geospatial data encoded in Geography Markup Language (GML).

© Copyright 2011-2022 National Emergency Number Association, Inc.

Term or Abbreviation (Expansion)	Definition / Description
WSDL (Web Service Definition Language)	The Web Services Description Language (WSDL) is an XML-based language used to describe the services a business offers and to provide a way for individuals and other businesses to access those services electronically. WSDL is the cornerstone of the Universal Description, Discovery, and Integration (UDDI) initiative spearheaded by Microsoft, IBM, and ARIBA. UDDI is an XML-based registry for businesses worldwide, which enables businesses to list themselves and their services on the Internet. WSDL is the language used to do this.. WSDL is derived from Microsoft's Simple Object Access Protocol (SOAP) and IBM's Network Accessible Service Specification Language (NASSL). WSDL replaces both NASSL and SOAP as the means of expressing business services in the UDDI registry. An XML-based interface definition language that is used for describing the functionality offered by a web service.
X.509	An ITU-T standard for a public key infrastructure (PKI) and Privilege Management Infrastructure (PMI). In NG9-1-1, refers to the format of a certificate containing a public key.
XACML (eXtensible Access Control Markup Language)	A general-purpose access control policy language that provides an XML-based syntax for defining rules to control access to resources.
XML (eXtensible Markup Language)	An internet specification for web documents that enables tags to be used that provide functionality beyond that in Hyper Text Markup Language (HTML). Its reference is its ability to allow information of indeterminate length to be transmitted to a PSAP call taker or dispatcher versus the current restriction that requires information to fit the parameters of pre-defined fields.
XMPP (Extensible Messaging and Presence Protocol)	A standardized protocol for exchanging instant messages, presence, files, and other objects.
YAML (YAML Ain't Markup Language)	A human-readable data-serialization language; commonly used for configuration files and in applications where data is being stored or transmitted.

© Copyright 2011-2022 National Emergency Number Association, Inc.

12 References

Note that this version of the document contains some references to documents that are works in progress at the IETF and other organizations. This document may be revised as these references stabilize.

[1] National Emergency Number Association. *Master Glossary of 9-1-1 Terminology.* NENA-ADM-000.23-2020. Arlington, VA: NENA, approved January 20, 2020.

[2] National Emergency Number Association. *i3 Technical Requirements Document*. NENA 08-751. Arlington, VA: NENA, approved September 28, 2006.

[3] National Emergency Number Association. *Interim VoIP Architecture for Enhanced 9-1-1 Services (i2)*. NENA 08-001. Arlington, VA: NENA, approved August 11, 2010.

[4] Internet Engineering Task Force. *Framework for Emergency Calling in Internet Multimedia*. B. Rosen, J. Polk, H. Schulzrinne, and A. Newton. RFC 6443, December 2011.

[5] Internet Engineering Task Force. *Geopriv Requirements*. J. Cuellar, J. Morris, D. Mulligan, J. Peterson, and J. Polk. RFC 3693, February 2004.

[6] Internet Engineering Task Force. *A Presence-based GEOPRIV Location Object Format.* J. Peterson. RFC 4119, December 2005.

[7] Internet Engineering Task Force. *HTTP Enabled Location Delivery (HELD)*. M. Barnes, ed. RFC 5985, September 2010.

[8] Internet Engineering Task Force. *Session Initiation Protocol Location Conveyance*. J. Polk, B. Rosen and J. Peterson. RFC 6442, December 2011.

[9] Internet Engineering Task Force. *A Hitchhikers Guide to the Session Initiation Protocol (SIP)*. J. Rosenberg. RFC 5411, February 2009.

[10] Internet Engineering Task Force. *Session Initiation Protocol*. H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, E. Schooler. RFC 3261, June 2002.

[11] Internet Engineering Task Force. *RTP: A Transport Protocol for Real-Time Applications*. H. Schulzrinne, S. Casner, R. Frederick, and V. Jacobson. RFC 3550, July 2003.

[12] Internet Engineering Task Force. *SDP: Session Description Protocol*. J. Handley, V. Jacobson, and C. Perkins. RFC 4566, July 2006.

[13] Internet Engineering Task Force. *Session Initiation Protocol (SIP): Locating SIP Servers*. J. Rosenberg and H. Schulzrinne. RFC 3263, June 2002.

[14] Internet Engineering Task Force. *Session Initiation Protocol (SIP)-Specific Event Notification*. A. Roach. RFC 6665, July 2012.

[15] Internet Engineering Task Force. *The Session Initiation Protocol UPDATE Method*. J. Rosenberg. RFC 3311, September 2002.

© Copyright 2011-2022 National Emergency Number Association, Inc.

[16] Internet Engineering Task Force. *Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks*. C. Jennings, J. Peterson, and M. Watson. RFC 3325, November 2002.
[17] Internet Engineering Task Force. *Session Initiation Protocol (SIP) Extension for Instant Messaging*. B. Campbell, J. Rosenberg, H. Schulzrinne, C. Huitema, and D. Gurle. RFC 3428, December 2002.
[18] Internet Engineering Task Force. *The Reason Header Field for the Session Initiation Protocol (SIP)*. H. Schulzrinne, D. Oran, and G. Camarillo. RFC 3326, December 2002.
[19] Internet Engineering Task Force. *The Session Initiation Protocol (SIP) Refer Method*. R. Sparks. RFC 3515, April 2003.
[20] Internet Engineering Task Force. *Grouping of Media Lines in the Session Description Protocol (SDP)*. G. Camarillo and H. Schulzrinne. RFC 5888, June 2010.
[21] Internet Engineering Task Force. *An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing*. J. Rosenberg and H. Schulzrinne. RFC 3581, August 2003.
[22] Internet Engineering Task Force. *Real-time Control Protocol (RTCP) attribute in Session Description Protocol (SDP)*. C. Huitema. RFC 3605, October 2003.
[23] Internet Engineering Task Force. *Indicating User Agent Capabilities in the Session Initiation Protocol (SIP)*. J. Rosenberg, H. Schulzrinne, and P. Kyzivat. RFC 3840, August 2004.
[24] Internet Engineering Task Force. *Caller Preferences for the Session Initiation Protocol (SIP)*. J. Rosenberg, H. Schulzrinne, and P. Kyzivat. RFC 3841, August 2004.
[25] Internet Engineering Task Force. *A Presence Event Package for the Session Initiation Protocol (SIP)*. J. Rosenberg. RFC 3856, August 2004.
[26] Internet Engineering Task Force. *A Watcher Information Event Template-Package for the Session Initiation Protocol (SIP)* J. Rosenberg. RFC 3857, August 2004.
[27] Internet Engineering Task Force. *The Session Initiation Protocol (SIP) "Replaces" Header*. R. Mahy, B. Biggs, and R. Dean. RFC 3891, September 2004.
[28] Internet Engineering Task Force. *The Session Initiation Protocol (SIP) Referred-By Mechanism*. R. Sparks. RFC 3892, September 2004.
[29] Internet Engineering Task Force. *Using E.164 numbers with the Session Initiation Protocol (SIP)*. J. Peterson, H. Liu, J. Yu, and B. Campbell. RFC 3824, June 2004.
[30] Internet Engineering Task Force. *Early Media and Ringing Tone Generation in the Session Initiation Protocol (SIP)*. G. Camarillo and H. Schulzrinne. RFC 3960, December 2004.
[31] Internet Engineering Task Force. *Presence Information Data Format (PIDF)*. H. Sugano, S. Fujimoto, G. Klyne, A. Bateman, and J. Peterson. RFC 3863, August 2004.

© Copyright 2011-2022 National Emergency Number Association, Inc.

[32] Internet Engineering Task Force. *Session Timers in the Session Initiation Protocol (SIP)*. S. Donovan and J. Rosenberg. RFC 4028, April 2005.
[33] Internet Engineering Task Force. *Internet Media Type message/sipfrag*. R. Sparks. RFC 3420, November 2002.
[34] Internet Engineering Task Force. *Basic Network Media Services with SIP*. J. Berger, Ed., J. Van Dyke, and A. Spitzer. RFC 4240, December 2005.
[35] Internet Engineering Task Force. *An Extension to the Session Initiation Protocol (SIP) for Request History Information*. M. Barnes, F. Audet, S. Schubert, J. van Elburg, and C. Holmberg. RFC 7044, February 2014.
[36] Internet Engineering Task Force. *Actions Addressing Identified Issues with the Session Initiation Protocol's (SIP) Non-INVITE Transaction*. R. Sparks. RFC 4320, January 2006.
[37] Internet Engineering Task Force. *Communications Resource Priority for the Session Initiation Protocol (SIP)*. H. Schulzrinne, and J. Polk. RFC 4412, February 2006.
[38] Internet Engineering Task Force. *Conveying Feature Tags with the Session Initiation Protocol (SIP) REFER Method*. O. Levin, and A. Johnston. RFC 4508, May 2006.
[39] Internet Engineering Task Force. *Session Initiation Protocol Call Control - Conferencing for User Agents*. A. Johnston and O. Levin. RFC 4579, August 2006.
[40] Internet Engineering Task Force. *A Session Initiation Protocol (SIP) Event Package for Conference State*. R. Rosenberg, H. Schulzrinne, and O. Levin. RFC 4575, August 2006.
[41] Internet Engineering Task Force. *Obtaining and Using Globally Routable User Agent (UA) URIs (GRUU) in the Session Initiation Protocol (SIP)*, J. Rosenberg, Internet Engineering Task Force, RFC 5627, October 2009.
[42] Internet Engineering Task Force. *Managing Client-Initiated Connections in the Session Initiation Protocol (SIP)*. C. Jennings, Ed., R. Mahy, Ed., and F. Audet, Ed.. RFC 5626, October 2009.
[43] Internet Engineering Task Force. *Session Initiation Protocol Package for Voice Quality Reporting*. A. Pendleton, A. Clark, A. Johnston, and H. Sinnreich. RFC 6035, November 2010.
[44] Internet Engineering Task Force. *Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols*. A. Keranen, C. Holmberg, and J. Rosenberg. RFC 8445, July 2018.
[45] Internet Engineering Task Force. *A Uniform Resource Name (URN) for Emergency and Other Well-Known Services*. H. Schulzrinne. RFC 5031, January 2008.
[46] Internet Engineering Task Force. *Best Current Practice for Communications Services in support of Emergency Calling*. B. Rosen and J. Polk. RFC 6881, March 2013.
[47] Internet Engineering Task Force. *Location-to-URL Mapping Architecture and Framework*. H. Schulzrinne. RFC 5582, September 2009.

© Copyright 2011-2022 National Emergency Number Association, Inc.

[48] Internet Engineering Task Force. *LoST: A Location-to-Service Translation Protocol.* T. Hardie, A. Newton, H. Schulzrinne, and H. Tschofenig. RFC 5222, August 2008.
[49] 3rd Generation Partnership Project. *IP Multimedia Subsystem (IMS) emergency sessions*. Curt Wong. 3GPP TS 23.167, January 22, 2015.
[50] Telecommunications Industry Association and Alliance for Telecommunications Industry Solutions. *Enhanced Wireless 9-1-1 Phase 2*. Washington, DC: ATIS. J-STD-036-C-2. Washington, DC: ATIS, June 2017.
[51] Organization for the Advancement of Structured Information Standards (OASIS). *Universal Description, Discovery, and Integration (UDDI) Version 3.0*. L. Clement, A. Hately, C. von Riegen, T. Rogers. UDDI V3.0, October 19, 2004.
[52] Internet Engineering Task Force. *GEOPRIV Presence Information Data Format Location Object (PIDF-LO) Usage Clarification, Considerations, and Recommendations*. J. Winterbottom, M. Thomson, and H. Tschofenig. RFC 5491, March 2009.
[53] Internet Engineering Task Force. *Revised Civic Location Format for Presence Information Data Format Location Object (PIDF-LO)*. M. Thomson and J. Winterbottom. RFC 5139, March 2009.
[54] Internet Engineering Task Force. *Requirements for a Location-by-Reference Mechanism used in Location Configuration and Conveyance*. R. Marshall. RFC 5808, May 2010.
[55] Internet Engineering Task Force. A Location Dereferencing Protocol Using HTTP-Enabled Location Delivery (HELD), J. Winterbottom, H. Tschofenig, H. Schulzrinne, and M. Thomson. RFC 6753, October 2012.
[56] Internet Engineering Task Force. *Session Initiation Protocol (SIP) Overload Contro*. V. Gurbani, V. Hilt, and H. Schulzrinne. RFC 7339, September 2014.
[57] Internet Engineering Task Force. *The Transport Layer Security (TLS) Protocol Version 1.1*. T. Dierks and E. Rescola. RFC 4346, April 2006.
[58] Organization for the Advancement of Structured Information Standards (OASIS). *Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0*. S. Cantor, J. Kemp, R. Philpott, and E. Maler. saml-core-2.0-os, March 15, 2005.
[59] Internet Engineering Task Force. *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*. S. Chokani, W. Ford, R. Sabett, C. Merrill, and S. Wu. RFC 3647, November 2003.
[60] Internet Engineering Task Force. *Authenticated Identity Management in the Session Initiation Protocol (SIP)*. J. Peterson, C. Jennings, E. Rescorla, and C. Wendt. RFC 8224, February 2018.

© Copyright 2011-2022 National Emergency Number Association, Inc.

[61] Organization for the Advancement of Structured Information Standards (OASIS). *eXtensible Access Control Markup Language (XACML) Version 2.0*. XACML 2.0, February 1, 2005.
[62] National Institute of Standards and Technology. *Secure Hash Standard, Federal Information Processing Standards Publication 180-4.* FIPS-PUB-180-4, August 2015.
[63] National Institute of Standards and Technology. *Advanced Encryption Standard, Federal Information Processing Standards Publication 197*. FIPS-PUB-197, November 26, 2001.
[64] Internet Engineering Task Force. *Simple Network Management Protocol, Version 3 (SNMPv3)*. J. Case, R. Mundy, D. Partain, and B. Stewart. RFC 3410, December 2002 through RFC 3418, December 2002.
[65] Internet Engineering Task Force. *RTP Control Protocol Extended Reports (RTCP XR)*. T. Friedman, Ed., R. Caceres, Ed., and A. Clark, Ed. RFC 3611, November 2003.
[66] Organization for the Advancement of Structured Information Standards. *Common Alerting Protocol V1.0*. A. Botterell. oasis-200402-cap-core-1.0, March 2004.
[67] National Institute of Standards and Technology. *Security Requirements for Cryptographic Modules, Federal Information Processing Standards Publication 140-2*. FIPS-PUB-140-3, March 22, 2019.
[68] Internet Engineering Task Force. *An INVITE-Initiated Dialog Event Package for the Session Initiation Protocol (SIP). J. Rosenberg, H. Schulzrinne, and R. Mahy*. RFC 4235, November 2005.
[69] GML 3.1.1 PIDF-LO Shape Application Schema for Use by the Internet Engineering Task Force (IETF), M. Thomson and C. Reed, Candidate OpenGIS Implementation Specification 06-142r1, Version 1.0, April 2007.
[70] National Emergency Number Association. *Functional and Interface Standards for Next Generation 9-1-1 Version 1.0 (i3)*. NENA 08-002. Arlington, VA: NENA, approved December 18, 2007.
[71] National Emergency Number Association. *Technical Information Document Network/System Access Security*. NENA 04-503. Arlington, VA: NENA, approved December 1, 2005.
[72] Internet Engineering Task Force. *Filtering Location Notifications in the Session Initiation Protocol (SIP)*. R. Mahy, B. Rosen, and H. Tschofenig. RFC 6447, January 2012.
[73] National Emergency Number Association. *NG9-1-1 Additional Data*. NENA-STA-012.2-2017. Arlington, VA: NENA, approved December 21, 2017.
[74] Internet Engineering Task Force. *Domain Names – Concepts And Facilities.* , P. Mockapetris. RFC 1034, November 1987.
[75] Internet Engineering Task Force. *A DNS RR for specifying the location of services (DNS SRV)*. A. Gulbrandsen, P. Vixie, and L. Esibov. RFC 2782, February 2000.

© Copyright 2011-2022 National Emergency Number Association, Inc.

[76] SIPforum. *IP PBX / Service Provider Interoperability.* C. Sibley, C. Gatch. SIPconnect Technical Recommendation V1.0, January 23, 2008.
[77] National Emergency Number Association. *Next Generation United States Civic Location Data Exchange Format (CLDXF)*. NENA-STA-004.1-2014, Arlington, VA: NENA, approved March 23, 2014.
[78] Organization for the Advancement of Structured Information Standards. *Emergency Data Exchange Language Distribution Element (EDXL-DE) 1.0*. M. Raymond, S. Webb, and P. Aymond. OASIS EDXL-DE v1.0, May 1, 2006.
[79] Internet Engineering Task Force. *Synchronizing Service Boundaries and <mapping> Elements Based on the Location-to-Service Translation (LoST) Protocol*. H. Schulzrinne and H. Tschofenig. RFC 6739, October 2012.
[80] Internet Engineering Task Force. *Session Initiation Protocol (SIP) Event Notification Extension for Notification Rate Control*. A. Niemi, K. Kiss, and S. Loreto. RFC 6446, January 2012.
[81] Internet Engineering Task Force. *Design Considerations for Session Initiation Protocol (SIP) Overload Control*. V. Hilt, E. Noel, C. Shen, and A. Abdelai. RFC 6357, August 2011.
[82] World Wide Web Consortium (W3C). *XML Schema Part 2: Datatypes Second Edition*. P. Biron and A. Malhotra. http://www.w3.org/TR/xmlschema-2/, October 28, 2004.
[83] Internet Engineering Task Force. *Session Traversal Utilities for NAT (STUN)*, J. Rosenberg, R. Mahy, P. Matthews, and D. Wing. RFC 5389, October 2008.
[84] Internet Engineering Task Force. *Framework for Real-Time Text over IP Using the Session Initiation Protocol (SIP)*. A. van Wijk and G. Gybels. RFC 5194, June 2008.
[85] Internet Engineering Task Force. *RTP Payload for Text Conversation*. G. Hellstrom and P. Jones. RFC 4103, June 2005.
[86] Internet Engineering Task Force. *Framework for Transcoding with the Session Initiation Protocol (SIP)*. G. Camarillo. RFC 5369, October 2008.
[87] Internet Engineering Task Force. *Indication of Message Composition for Instant Messaging*. H. Schulzrinne. RFC 3994, January 2005.
[88] Internet Engineering Task Force. *The Message Session Relay Protocol (MSRP)*. B. Campbell, Ed., R. Mahy, Ed., and C. Jennings, Ed. RFC 4975, September 2007.
[89] Internet Engineering Task Force. *Relay Extensions for the Message Session Relay Protocol (MSRP)*. C. Jennings, R. Mahy, A.B. Roach, Internet Engineering Task Force, RFC 4976, September 2007.
[90] Internet Engineering Task Force. *Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types*. N. Freed and N. Borenstein. RFC 2046, November 1996.
[91] Alliance for Telecommunications Industry Solutions. *Signalling System Number 7 (SS7) – Operator Services Network Capabilities*. ATIS-1000666.1999 (S2019). Washington, DC: ATIS, February 11, 1999.

© Copyright 2011-2022 National Emergency Number Association, Inc.

[92] Internet Engineering Task Force. *An Extensible Markup Language (XML)-Based Format for Event Notification Filters*. H. Khartabil, E. Leppanen, M. Lonnfors, and J. Costa-Requena. RFC 4661, September 2006.

[93] Open Geospatial Consortium. *OGC Web Feature Service 2.0 Interface Standard – With Corrigendum Version 2.0.2*. P. Vretanos. OGC09-025r2, July 10, 2014.

[94] Open Geospatial Consortium. *OWS 7 Engineering Report – Geosynchronization service*. P. Vretanos, , OGC 10-069r2, January 12, 2011.

[95] Internet Engineering Task Force. *The Atom Syndication Format*. M. Nottingham and R. Sayre. RFC 4287, December 2005.

[96] Internet Engineering Task Force. *The ATOM Publishing Protocol*. J. Gregorio, Ed., and B. de hOra, Ed. RFC 5023, October 2007.

[97] World Wide Web Consortium. *Voice Extensible Markup Language (VoiceXML) Version 2.0*. S. McGlashan, D. Burnett, J. Carter, P. Danielsen, J. Ferrans, A. Hunt, B. Lucas, B. Porter, K. Rehor, and S. Tryphonas. REC-voicexml20-20040316, 16 March 2004.

[98] Internet Engineering Task Force. *Real-time Streaming Protocol Version 2.0*. H. Schulzrinne, A. Rao, R. Lanphier, M. Westerlund, and M. Stiemerling, Ed., RFC 7826, December 2016.

[99] Internet Engineering Task Force. *The Session Description Protocol (SDP) Label Attribute*. O. Levin and G. Camarillo, RFC 4574, August 2006.

[100] Internet Engineering Task Force. *An Extension to the Session Description Protocol (SDP) and Real-time Transport Protocol (RTP) for Media Loopback*. H. Kaplan, K. Hedayat, N. Venna, P. Jones, and N. Stratton. RFC 6849, February 2013.

[101] 3rd Generation Partnership Project 2. *Enhanced Variable Rate Codec, Speech Service Option 3 for Wideband Spread Spectrum Digital Systems*. C.S0014-A V1.0, April 2004; and also Internet Engineering Task Force. *RTP Payload Format for Enhanced Variable Rate Codecs (EVRC) and Selectable Mode Vocoders (SMV)*. A. Li. RFC 3558, July 2003.

[102] 3rd Generation Partnership Project 2. *Enhanced Variable Rate Codec, Speech Service Option 3 and 68 for Wideband Spread Spectrum Digital Systems.* C.S0014-B V1.0, May 2006; and also Internet Engineering Task Force. *Enhancements to RTP Payload Formats for EVRC Family Codecs*. Q. Xie and R. Kapoor. RFC 4788, January 2007.

[103] 3rd Generation Partnership Project 2. *Enhanced Variable Rate Codec, Speech Service Options 3, 68, and 70 for Wideband Spread Spectrum Digital Systems*. C.S0014-C V1.0, January 2007; and also Internet Engineering Task Force. *RTP Payload Format for the Enhanced Variable Rate Wideband Codec (EVRC-WB) and the Media Subtype Updates for EVRC-B Codec*. H. Desineni and Q. Xie. RFC 5188, February 2008.

[104] 3rd Generation Partnership Project 2. *Enhanced Variable Rate Codec, Speech Service Options 3, 68, 70, and 73 for Wideband Spread Spectrum Digital Systems*. C.S0014-D V1.0, May 2009; and also Internet Engineering Task Force. *RTP payload*

© Copyright 2011-2022 National Emergency Number Association, Inc.

format for Enhanced Variable Rate Narrowband-Wideband Codec (EVRC-NW). R. Aggarwal, K. Kompella, T. Nadeau, and G. Swallow. RFC 6884, June 2010.

[105] National Emergency Number Association. "Funding 9-1-1 Into the Next Generation: An Overview of NG9-1-1 Funding Model Options for Consideration". NG Funding Report. Arlington, VA: NENA, March 2007.

[106] National Emergency Number Association. "Next Generation 9-1-1 Transition Policy Implementation Handbook: A Guide for Identifying and Implementing Policies to Enable NG9-1-1". NG911 Transition Policy Handbook. Arlington, VA: NENA, March 2010.

[107] Internet Engineering Task Force. *Additional Data related to an Emergency Call*. R. Gellens, B. Rosen, H. Tschofenig, R. Marshall, and J. Winterbottom. RFC 7852, July 2016.

[108] Internet Engineering Task Force. *Geolocation Policy: A Document Format for Expressing Privacy Preferences for Location Information*. H. Schulzrinne, H. Tschofenig, J. Cuellar, J. Polk, J. Morris, and M. Thomson. RFC 6772, January 2013.

[109] Internet Engineering Task Force. *Common Policy: A Document Format for Expressing Privacy Preferences*.. H. Schulzrinne, H. Tschofenig, J. Morris, J. Cuellar, J. Polk, J. Rosenberg. RFC 4745, February 2007.

[110] National Institute of Standards and Technology. *Guide to Storage Encryption Technologies for End User Devices*. K. Scarfone, M. Souppaya, and M. Sexton. NIST Special Publication 800-111, November 2007.

[111] National Emergency Number Association. *Emergency Incident Data Object (EIDO)*. NENA-STA-021.1-201X. Arlington, VA: NENA (forthcoming).

[112] Internet Engineering Task Force. *URN Syntax*. R. Moats. RFC 2141, <date>.

[113] Internet Engineering Task Force. *xCard: vCard XML Representation*. S. Perreault. RFC 6351, May 1997.

[114] National Emergency Number Association *Legacy Selective Router Gateway Technical Standard.* NENA-STA-034.1-202x. Arlington, VA: NENA, (forthcoming).

[115] Internet Engineering Task Force. *Specifying Civic Address Extensions in the Presence Information Data Format Location Object (PIDF-LO)*. J. Winterbottom, M. Thomson, R. Barnes, B. Rosen, and R. George. RFC 6848, January 2013.

[116] Internet Engineering Task Force. *Session Recording Protocol*. L. Portman, H. Lum, Ed., C. Eckel, A. Johnston, and A. Hutton. RFC 7866, May 2016.

[117] Internet Engineering Task Force. *Session Initiation Protocol (SIP) Recording Metadata*. R. Mohan, P. Ravindran, and P. Kyzivat. RFC 7865, May 2016.

[118] Internet Engineering Task Force. *DNS Security Introduction and Requirements*. R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose. RFC 4035, March 2005.

© Copyright 2011-2022 National Emergency Number Association, Inc.

[119] Internet Engineering Task Force. *Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN)*. R. Mahy, P. Matthews, and J. Rosenberg. RFC 5766, April 2010.
[120] International Telecommunications Union. *The international public telecommunication numbering plan*. Recommendation E.164 (11/10), November 18, 2010.
[121] Internet Engineering Task Force. *Codec Control Messages in the RTP Audio-Visual Profile with Feedback (AVPF)*. S. Wenger, U. Chandra, M. Westerlund, and B. Burman. RFC 5104, February 2008.
[122] Internet Engineering Task Force. *XML Schema for Media Control.* O. Levin, R. Even, and P. Hagendorf. RFC 5168, March 2008.
[123] Internet Engineering Task Force. *Multi-party Chat Using the Message Session Relay Protocol (MSRP)*. A. Niemi, M. Garcia-Martin, and G. Sandbakken. RFC 7701, December 2015.
[124] Internet Engineering Task Force. *Extended RTP Profile for Real-time Transport Control Protocol (RTCP)-Based Feedback (RTP/AVPF)*. J. Ott, S. Wenger, N. Sato, C. Burmeister, and J. Rey. RFC 4585, July 2006.
[125] Internet Engineering Task Force. *Call Processing Language (CPL): A Language for User Control of Internet Telephony Services*. J. Lennox, X. Wu, and H. Schulzrinne. RFC 3880, October 2004.
[126] Internet Engineering Task Force. *Uniform Resource Identifier (URI): Generic Syntax.* T. Berners-Lee, R. Fielding and L. Masinter. RFC 3986, January 2005.
[127] Organization for the Advancement of Structured Information Standards (OASIS). *Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0*. saml-bindings-2.0-os, March 15, 2005.
[128] Organization for the Advancement of Structured Information Standards (OASIS). *Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0.* saml-profiles-2.0-os, March 15, 2005.
[129] Organization for the Advancement of Structured Information Standards (OASIS). *Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0*. saml-metadata-2.0-os, March 15, 2005.
[130] Alliance for Telecommunications Industry Solutions. *Interworking between Session Initiation Protocol (SIP) and Bearer Independent Call Control or ISDN User Part*. ATIS 1000679.2015. Washington, DC: ATIS, April 14, 2015.
[131] Internet Engineering Task Force. *Discovering Location-to-Service Translation (LoST) Servers Using the Dynamic Host Configuration Protocol (DHCP)*. H. Schulzrinne, J. Polk, and H. Tschofenig. RFC 5223, August 2008.
[132] Internet Engineering Task Force. *Content-ID and Message-ID Uniform Resource Locators*. E. Levinson. RFC 2392, August 1998.

© Copyright 2011-2022 National Emergency Number Association, Inc.

[133] Internet Engineering Task Force. *Simple Mail Transfer Protocol*. J. Klensin. RFC 5321, October 2008.
[134] Internet Engineering Task Force. *An Architecture for Differentiated Services*, S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang and W. Weiss. RFC 2475, December 1998.
[135] Internet Engineering Task Force. *Date and Time on the Internet: Timestamps*. G. Klyne and C. Newman. RFC 3339, July 2002.
[136] Alliance For Telecommunications Industry Solutions. *ECS – Connection and Ring Back Addendum [Supplement to ATIS-1000628.2000 (R2010)]*, ATIS-1000678.a.2001(R2015). Washington, DC: ATIS, August 2002.
[137] Cable Television Laboratories, Inc. *Residential SIP Telephony Feature Specification*. PKT-SP-RSTF-C01-140314, March 14, 2014.
[138] Cable Television Laboratories, Inc. *CMS to CMS Signaling Specification*. PKT-SP-CMSS1.5-I07-120412, April 12, 2012.
[139] Internet Engineering Task Force. *Integrated Services Digital Network (ISDN) User Part (ISUP) to Session Initiation Protocol (SIP) Mapping*. G. Camarillo, A. B. Roach, J. Peterson, and L. Ong. RFC 3398, December 2002.
[140] Internet Engineering Task Force. *Definition of Events for Channel-Oriented Telephony Signalling*. H. Schulzrinne and T. Taylor. RFC 5244, June 2008.
[141] Internet Engineering Task Force. *Public Safety Answering Point (PSAP) Callback*. H. Schulzrinne, H. Tschofenig, C. Holmberg, and M. Patel. RFC 7090, April 2014.
[142] Internet Engineering Task Force. *RTP Payload for DTMF Digits, Telephony Tones, and Telephony Signals*. H. Schulzrinne and T. Taylot. RFC 4733, December 2006.
[143] Telcordia Technologies. *Telcordia Technologies Specification of Signalling System Number 7*. GR-246-CORE, December 2005.
[144] International Telecommunications Union. *The Directory: Public-key and attribute certificate frameworks*. Recommendation X.509 (10/2019), October 14, 2019.
[145] Internet Engineering Task Force. *Representation of Uncertainty and Confidence in the Presence Information Data Format Location Object (PIDF-LO)*. M. Thomson and J. Winterbottom. RFC 7459, February 2015.
[146] Internet Engineering Task Force. *Dynamic Extensions to the Presence Information Data Format Location Object (PIDF-LO)*. H. Schulzrinne, V. Singh, H. Tschofenig, and M. Thomson. RFC 5962, September 2010.
[147] Internet Engineering Task Force. *Dynamic Host Configuration Protocol*. R. Droms. RFC 2131, March 1997.
[148] World Wide Web Consortium (W3C). *SOAP Version 1.2 Part 1: Messaging Framework (Second Edition)*. M. Gugin, M. Hadley, N. Mendelsohn, J-J. Moreau, H. F. Nielsen, A. Karmarkar, and Y. Lafon. TR/2007/REC-soap12-part1-20070427, April 27, 2007.

© Copyright 2011-2022 National Emergency Number Association, Inc.

[149] Internet Engineering Task Force. *Session Initiation Protocol (SIP) INFO Method and Package Framework*. C. Holmberg, E. Burger, and H. Kaplan. RFC 6086, January 2011.
[150] Internet Engineering Task Force. *The tel URI for Telephone Numbers*. H. Schulzrinne. RFC 3966, December 2004.
[151] Alliance For Telecommunications Industry Solutions. *ATIS Standard for Implementation of 3GPP Common IMS Emergency Procedures for IMS Origination and ESInet/Legacy Selective Router Termination*. ATIS-0700015.v004. Washington, DC: ATIS, July 2018.
[152] Association of Public-Safety Communications Officials (APCO) and Central Station Alarm Association (CSAA). *Alarm Monitoring Company to Public Safety Answering Point (PSAP) Computer-Aided Dispatch (CAD) Automated Secure Alarm Protocol (ASAP)*, APCO/CSAA ANS 2.101.2-2014, August 5, 2014.
[153] Internet Engineering Task Force. *HTTP over TLS*. E. Rescorla. RFC 2818, May 2000.
[154] Internet Engineering Task Force. *Domain-Based Application Service Location Using URIs and the Dynamic Delegation Discovery Service (DDDS)*. L. Daigle. RFC 4848, April 2007.
[155] Internet Engineering Task Force. *Discovering the Local Location Information Server (LIS)*. M. Thomson and J. Winterbottom. RFC 5986, September 2010.
[156] Internet Engineering Task Force. *A Session Initiation Protocol (SIP) Event Package for Key Press Stimulus (KPML)*. E. Burger and M. Dolly. RFC 4730, November 2006.
[157] International Organization for Standardization (ISO).*Identification cards – Integrated circuit cards.* ISO/IEC 7816 (1-15). Geneva: ISO, 1999-2018.
[158] Internet Engineering Task Force. *Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.2*. K. Moriarty, Ed., B. Kaliski, J. Jonsson, and A. Rusch. RFC 8017, November 2016.
[159] Telcordia Technologies. *CCS/SS7 Generic Requirements in Support of E9-1-1 Service*. GR-2956-CORE, December 2002.
[160] Telcordia Technologies. *LSSGR: Switching System Generic Requirements for Call Control Using the Integrated Services Digital Network User Part (ISDNUP)*. GR-317-CORE, November 2007.
[161] Internet Engineering Task Force. *Representing Trunk Groups in tel/sip Uniform Resource Identifiers (URIs)*. V. Gurbani and C. Jennings. RFC 4904, June 2007.
[162] Internet Engineering Task Force. *Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing*. R. Fielding, Ed. and J. Reschke, Ed. RFC 7230, June 2014.
[163] National Emergency Number Association. *NENA Standard for the implementation of Enhanced MF Signaling, E9-1-1 Tandem to PSAP*. NENA 03-002. Arlington, VA: NENA, January 17, 2007.

© Copyright 2011-2022 National Emergency Number Association, Inc.

[164] National Emergency Number Association. *NENA E9-1-1 PSAP Equipment Standards*. NENA-STA-027.3-2018 (originally 04-001). Arlington, VA: NENA, July 2, 2018.
[165] National Emergency Number Association. *NENA ALI Query Service Standard*. NENA 04-005, Arlington, VA: NENA, November 21, 2006.
[166] Internet Engineering Task Force. *Framework for Establishing a Secure Real-time Transport Protocol (SRTP) Security Context Using Datagram Transport Layer Security (DTLS)*. J. Fischl, H. Tschofenig, and E. Rescorla. RFC 5763, May 2010.
[167] Internet Engineering Task Force. *Datagram Transport Layer Security (DTLS) Extension to Establish Keys for the Secure Real-time Transport Protocol (SRTP)*. D. McGrew and E. Rescorla. RFC 5764, May 2010
[168] Internet Engineering Task Force. *Next-Generation Vehicle-Initiated Emergency Calls*. R. Gellens, B. Rosen, and H. Tschofenig. RFC 8148, May, 2017.
[169] Association of Public-Safety Communications Officials. *Vehicular Emergency Data Set (VEDS) Recommendation Version 3.0*. VEDS 3.0. Daytona Beach: Advanced Automatic Crash Notification (AACN) Joint APCO/NENA Data Standardization Working Group, July 2012.
[170] Internet Engineering Task Force. *Private Session Initiation Protocol (SIP) Proxy-to-Proxy Extensions for Supporting the PacketCable Distributed Call Signaling Architecture*. F. Andreasen, B. McKibben and B. Marshall. RFC 5503, March 2009.
[171] Internet Engineering Task Force. *JSON Web Signature (JWS)*. M. Jones, J. Bradley, and N. Sakimura. RFC 7515, May 2015.
[172] Internet Engineering Task Force. *Real-time text media handling in multi-party conferences.* G. Hellstrom. Draft-hellstrom-mmusic-multi-party-rtt-00, November 1, 2019.
[173] Internet Engineering Task Force. *Negotiating Human Language in Real-Time Communications*. R. Gellens. RFC 8373, May 2018.
[174] National Emergency Number Association. *TTY/TDD Communications Standard Operating Procedure Model Recommendation*. NENA-STA-037.2-2018 (originally 56-004). Arlington, VA: NENA, August 17, 2018.
[175] Federal Communications Commission. *Proposed procedures for the TTY as a text terminal in legacy 9-1-1 PSAPs without IP connection*. EAAC Report. Washington DC: Emergency Access Advisory Committee (EAAC) TTY Transition Report, June 14, 2013.
[176] Internet Engineering Task Force. *Common Profile For Instant Messaging (CPIM)*. J. Peterson. RFC 3860, August 2004.
[177] Internet Engineering Task Force. *Common Presence and Instant Messaging (CPIM): Message Format*. G. Klyne and D. Atkins. RFC 3862, August 2004.
[178] Internet Engineering Task Force. *Validation of Locations Around a Planned Change*, B. Rosen. draft-ecrit-lost-planned-changes (expired), July 18, 2016.

© Copyright 2011-2022 National Emergency Number Association, Inc.

[179] Internet Assigned Numbers Authority (IANA). "Emergency Call Data Types." Accessed December 29, 2019. IANA registry.
[180] Internet Assigned Numbers Authority (IANA). "Language Subtag Registry." Accessed December 29, 2019. IANA registry.
[181] Internet Assigned Numbers Authority (IANA). "Media types." Accessed December 29, 2019. IANA Registry.
[182] SIPforum. *SIP-PBX / Service Provider Interoperability.* A. Hutton and G. Salgueiro. SIPconnect 2.0 Technical Recommendation, Document Number: TWG 11, 2016.
[183] Telecommunications Industry Association. *A Frequency Shift Keyed Modem for Use on the Public Switched Telephone Network*. TIA-825 Revision A. Englewood, CO: TIA, April 2003.
[184] National Emergency Number Association. *NENA Standard for NG9-1-1 GIS Data Model*. NENA-STA-006.1-2018. Arlington, VA: NENA, June 16, 2018.
[185] National Emergency Number Association. *NENA Standard for the Conveyance of Emergency Incident Data Objects (EIDOs) between Next Generation (NG9-1-1) Systems and Applications*. NENA-STA-024.1-202X. Arlington, VA: NENA, (forthcoming)
[186] Open Geospatial Consortium. *Open GIS Web Map Server Implementation Specification, Version 1.3.0*. J. de la Beaujardiere, Ed. OGC 06-042. March 15, 2006.
[187] Spatial Reference. "EPSG Projection 4326 – WGS 84." Last revised August 27, 2007. http://spatialreference.org/ref/epsg/4326/
[188] Alliance For Telecommunications Industry Solutions. *Network to Customer Installation Interfaces – Enhanced 911 Analog Voicegrade PSAP Access Using Loop Reverse-Battery Signaling*. ATIS 0600414.1998 (R2007) Washington, DC: ATIS, March 1, 1998.
[189] Telcordia Technologies. *E911 Public Safety Answering Point: Interface Between 1/1AESS Switch and Customer Premise Equipment.* GR-350-CORE, June 2003.
[190] Telcordia Technologies. *Enhanced MF Signaling: E9-1-1 Tandem to PSAP Interface*. GR-2953-CORE, March 1997.
[191] Alliance for Telecommunication Industry Solutions. *Joint ATIS/TIA Native SMS to 9-1-1 Requirements and Architecture Specification, Release 2*. ATIS J-STD-110.v002. Washington, DC: ATIS, May 1, 2015.
[192] Alliance for Telecommunication Industry Solutions. *Network to Customer Installation Interfaces – Enhanced 911 Analog Voicegrade PSAP Access Using Loop Reverse-*Battery Signaling. ATIS-0900414.2012(R2017). Washington, DC: ATIS, April 2012.
[193] National Emergency Number Association. *NENA Standard for NG9-1-1 Additional Data*. NENA STA-012.2.-2017 (originally 71-001). Arlington, VA: NENA, 12/21/2019.
[194] National Emergency Number Association. *NENA Registry System Standard*, NENA-STA-008.2-2014 (originally 70-001). Arlington, VA: NENA, October 6, 2014.

© Copyright 2011-2022 National Emergency Number Association, Inc.

[195] Internet Engineering Task Force. *Uniform Resource Name (URN) Namespace for the National Emergency Number Association (NENA)*. B. Rosen. RFC 6061, January 2011.
[196] Internet Engineering Task Force. *A Recommendation for Ipv6 Address Text Representation*. S. Kawamura and M. Kawashima. RFC 5952, August 2010.
[197] Internet Engineering Task Force. *Hypertext Transfer Protocol Version 2 (HTTP/2).* M. Belshe, R. Peon, and M. Thomson, Ed. RFC 7540, May 2015.
[198] Open Mobile Alliance. *Mobile Location Protocol 3.2 Approved Version 3.2*. OMA-TS-MLP-V3_2-20110719-A, July 19, 2011.
[199] Internet Engineering Task Force. *The Transport Layer Security (TLS) Protocol Version 1.2*. T. Dierks and E. Rescorla. RFC 5246, August 2008.
[200] Internet Engineering Task Force. *Transport Layer Security (TLS) Protocol Version 1.3*. E. Rescorla. RFC 8446, August 2018.
[201] Internet Engineering Task Force. *Location Source Parameter for the SIP Geolocation Header Field*. J. Winterbottom, R. Jesske, B. Chatras, and A. Hutton. RFC 8787. May 2020.
[202] Internet Engineering Task Force. *Next-Generation Pan-European eCall*. R. Gellens and H. Tschofenig. RFC 8147, May 2017.
[203] Internet Engineering Task Force. *PASSporT: Personal Assertion Token*. C. Wendt and J. Peterson. RFC 8225, February 2018.
[204] 3rd Generation Partnership Project. *Codec for Enhanced Voice Services (EVS)* J. Gibbs. 3GPP TS 26.441, June 2018.
[205] 3rd Generation Partnership Project. *Mandatory speech CODEC speech processing functions; AMR speech Codec; General Description.* S. Bruhn. 3GPP TS 26.071, June 2018.
[206] 3rd Generation Partnership Project. *Speech codec speech processing functions; Adaptive Multi-Rate - Wideband (AMR-WB) speech codec; ANSI-C code*. S. Bruhn. 3GPP TS 26.204, December 2018.
[207] Internet Engineering Task Force. *A Privacy Mechanism for the Session Initiation Protocol (SIP)*. J. Peterson. RFC 3323, November 2002.
[208] Internet Engineering Task Force. *P-Charge-Info: A Private Header Field (P-Header) Extension to the Session Initiation Protocol (SIP)*, D. York and T. Asversen. RFC 8496, October 2018.
[209] Internet Engineering Task Force. *Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3GPP*. R. Jesske, K. Drage, and C. Holmberg. et. al., RFC 7315, July 2014.
[210] Alliance for Telecommunications Industry Solutions and the SIP Forum. *Errata on ATIS Standard on Signature-based Handling of Asserted information using toKENs (SHAKEN).* ATIS-1000074-E. Washington, DC: ATIS, February 1, 2019.

© Copyright 2011-2022 National Emergency Number Association, Inc.

[211] Alliance for Telecommunications Industry Solutions and the SIP Forum. *Errata to ATIS Standard on Signature-based Handling of Asserted information using toKENs (SHAKEN): Governance Model and Certificate Management, Joint Alliance for Telecommunications Industry Solutions.* ATIS-1000080-E. Washington, DC: ATIS, approved February 27, 2019.
[212] Internet Engineering Task Force. *Definition of the Opus Audio Codec*. JM. Valin, K. Voss, and T. Terriberry. RFC 6716, September 2012.
[213] Internet Engineering Task Force. *The Use of AES-192 and AES-256 in Secure RTP*. D. McGrew. RFC 6188, March 2011.
[214] Internet Engineering Task Force. *Key words for use in RFCs to Indicate Requirement Levels*. S. Bradner. RFC 2119, March 1997.
[215] Internet Engineering Task Force. *jCard: The JSON Format for vCard*. P. Kewisch. RFC 7095, January 2014.
[216] Internet Engineering Task Force. *Network Time Protocol Version 4: Protocol and Algorithms Specification.* D. Mills, J. Marin, J. Burbank, and W. Kasch. RFC 5905, June 2010.
[217] Internet Engineering Task Force. *Connection Reuse in the Session Initiation Protocol (SIP).* V. Gurbani, R. Mahy, and B Tate. RFC 5923, June 2010.
[218] Internet Engineering Task Force. *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers.* K. Nichols, S. Blake, F. Baker, and D. Black. RFC 2474, December 1998.
[219] Internet Engineering Task Force. *RTP-mixer formatting of multi-party Real-time text*. G. Hellström. RFC 9071, July 2021.
[220] Internet Engineering Task Force. *Serving Stale Data to Improve DNS Resiliency.* D. Lawrence and W. Kumari, RFC 8767. March 2020.
[221] Internet Engineering Task Force. *JSON Web Algorithms (JWA).* M. Jones, RFC 7518. May, 2015.
[222] Internet Assigned Numbers Authority (IANA). *Hypertext Transfer Protocol (HTTP) Status Code Registry*. https://www.iana.org/assignments/http-status-codes/http-status-codes.xhtml, last updated 21 September 2018.
[223] Internet Engineering Task Force. *Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content.* R. Fielding, Ed. and J. Reschke, Ed. RFC 7231, June 2014.
[224] Internet Engineering Task Force. *The LoST-Validation S-NAPTR Application Service Tag*. R. Gellens and B. Rosen. RFC 8917, October 2020.
[225] Internet Engineering Task Force. *Non-interactive Emergency Calls.* B. Rosen, H. Schulzrinne, H. Tschofenig, and R. Gellens, RFC 8876. September 2020.
[226] 3rd Generation Partnership Project. *IP multimedia call control based on Session Initiation Protocol (SIP), Stage 3 (Release 17).* 3GPP. 3GPP TS 24.229, September 25, 2020.

© Copyright 2011-2022 National Emergency Number Association, Inc.

[227] Internet Engineering Task Force. *Edwards-Curve Digital Signature Algorithm (EdDSA)*. S. Josefsson and I. Liusvaara. RFC 8032, January 2017.
[228] Internet Engineering Task Force. *CFRG Elliptic Curve Diffie-Hellman (ECDH) and Signatures in JSON Object Signing and Encryption (JOSE)*. I. Liusvaara. RFC 8032, January 2017.
[229] Internet Engineering Task Force. *FYI on Questions and Answers – Answers to Commonly Asked "New Internet User" Questions.* R. Plzak, A. Wells, and A. Krol. RFC 2664, August 1999.
[230] National Emergency Number Association. *NENA Standard for the Implementation of the Wireless Emergency Service Protocol E2*, NENA-STA-018.2 (originally 05-001). Arlington, VA: NENA (forthcoming).
[231] National Emergency Number Association. *NENA Security for Next-Generation 9-1-1 Standard (NG-SEC),* NENA 71-001. Arlington, VA: NENA, February 6, 2010.
[232] National Emergency Number Association. "NENA Registry System". NRS Administrator. Updated September 30, 2020. http://technet.nena.org/nrs/registry/_registries.xml.
[233] Internet Engineering Task Force. *Dynamic Host Configuration Protocol for IPv6 (DHCPv6).* T. Mrugalski, M. Sidoleski, B. Volz, A. Yourtchenko, M. Richardson, S. Jiang, T. Lemon and T. Winters. RFC 8415, November 2018.
[234] Internet Engineering Task Force. *Path MTU Discovery for IP version 6.* J. McCann, S. Deering, J.Mogul, and R. Hinden, Ed. RFC 8201, July 2017.
[235] Internet Engineering Task Force. *Internet Control Message Protocol (ICMPv6 for the Internet Protocol Version 6 (IPv6) Specification.* A. Conta, S. Deering, and M. Gupta, Ed. RFC 4443, March 2006.

© Copyright 2011-2022 National Emergency Number Association, Inc.

Appendix A - Mapping Between NG9-1-1 and Legacy ALI Data Structures (Informative)

The following tables illustrate approximately equivalent legacy data elements and PIDF-LO/Additional Data Elements. Exact mapping of fields between legacy formats and NG formats is complex because local field usage in legacy systems varies widely, while field usage in NG9-1-1 is standardized and uniform. The LNG must map legacy elements to SIP header fields, PIDF-LO parameters, or Additional Data Elements (NENA 02-010 Field Name maps to PIDF-LO and/or Additional Data) for use within the NG9-1-1 system. The LPG must map SIP header fields, PIDF-LO parameters, or Additional Data Elements to legacy elements (PIDF-LO and/or Additional Data map to NENA 02-010 Field Name) for display in legacy PSAPs. The format of Table A-12-1 that is used in the "Standard ALI Query Best Practices" may be found on NENA.org.

Note: A future version of this document will further clarify how conversion between legacy formats and NG9-1-1 formats is accomplished.

NENA AQS Element	NG9-1-1 Mapping
Call Info	
CallBackNum	SIP INVITE/P-Asserted-Identity (P-A-I)[82] SIP INVITE/P-Preferred-Identity (P-P-I) for Non Service Initiated calls
CallingPartyNum (ANI)	SIP INVITE/P-Asserted-Identity (P-A-I) [70]
ClassOfService	Included in Additional Data and PIDF-LO. See Table A-12-2
TypeOfService	See Table A-12-3
SourceOfService	N/A
MainTelNum	EmergencyCallData.SubscriberInfo/SubscriberData/vcard/tel[n]/uri=tel : URI with MainTelNum expressed as a global number (i.e. starting with +1) AND EmergencyCallData:SubscriberInfo/ SubscriberData /vcard/tel[n]/parameters/type/text=main-number
CustomerName	EmergencyCallData:SubscriberInfo/ SubscriberData /vcard/fn/text= Full name of the customer
CustomerCode	N/A
AttentionIndicator	N/A
SpecialMessage	N/A

[82] CBN and CPN are assumed to be mutually exclusive. For Legacy to i3, both map to P-A-I. For i3 to Legacy, map P-A-I to CPN.

© Copyright 2011-2022 National Emergency Number Association, Inc.

NENA AQS Element	NG9-1-1 Mapping
AlsoRingsAtAddress	N/A
Location Info: StreetAddress	
HouseNum	pidflo:presence/tuple/status/geopriv/location-info/civicAddress/HNO
HouseNumSuffix	pidflo:presence/tuple/status/geopriv/location-info/civicAddress/HNS
PrefixDirectional	pidflo:presence/tuple/status/geopriv/location-info/civicAddress/PRD
StreetName	pidflo:presence/tuple/status/geopriv/location-info/civicAddress/RD
StreetSuffix	pidflo:presence/tuple/status/geopriv/location-info/civicAddress/STS
PostDirectional	pidflo:presence/tuple/status/geopriv/location-info/civicAddress/POD
TextualAddress	N/A
MSAGCommunity	[Mapped via MCS] pidflo:presence/tuple/status/geopriv/location-info/civicAddress/A3
PostalCommunity	pidflo:presence/tuple/status/geopriv/location-info/civicAddress/PCN
StateProvince	pidflo:presence/tuple/status/geopriv/location-info/civicAddress/A1
CountyID	[Mapped via MCS] pidflo:presence/tuple/status/geopriv/location-info/civicAddress/A2
Country	pidflo:presence/tuple/status/geopriv/location-info/civicAddress/country
TARCode	[Mapped via MCS]
PostalZipCode	pidflo:presence/tuple/status/geopriv/location-info/civicAddress/PC
Building	pidflo:presence/tuple/status/geopriv/location-info/civicAddress/BLD
Floor	pidflo:presence/tuple/status/geopriv/location-info/civicAddress/FLR
UnitNum	pidflo:presence/tuple/status/geopriv/location-info/civicAddress/UNIT The UnitNum and UnitType are combined in a PIDF-LO Unit with a separator. Examples include "Apartment 6", "Silver Suite", and "Gate 5". A Unit Num without a Unit Type or vice versa (for example "Penthouse") can also occur.
UnitType	pidflo:presence/tuple/status/geopriv/location-info/civicAddress/UNIT The UnitNum and UnitType are combined in a PIDF--LO Unit with a separator. Examples include "Apartment 6", "Silver Suite", and "Gate 5". A Unit Num without a Unit Type or vice versa (for example "Penthouse") can also occur.
LocationDescription	pidflo:presence/tuple/status/geopriv/location-info/civicAddress/LOC
LandmarkAddress	pidflo:presence/tuple/status/geopriv/location-info/civicAddress/LMK

© Copyright 2011-2022 National Emergency Number Association, Inc.

NENA AQS Element	NG9-1-1 Mapping
Location Info: Geo Location	
Latitude	pidflo:presence/tuple/status/geopriv/location-info/Circle/gml:pos [latitude part] OR pidflo:presence/tuple/status/geopriv/location-info/Sphere/gml:pos [latitude part]
Longitude	pidflo:presence/tuple/status/geopriv/location-info/Circle/gml:pos [longitude part] OR pidflo:presence/tuple/status/geopriv/location-info/Sphere/gml:pos [longitude part]
Elevation	pidflo:presence/tuple/status/geopriv/location-info/Sphere/gml:pos [altitude part]
Datum	Datum must always be WGS84 (EPSG4326/EPSG4979). Entities receiving locations with any other datum must convert the locations. The GML object (point, circle, polygon, etc.) in a PIDF-LO carries the datum, but the PIDF-LO and NENA Standard restrict to WGS84 only.
Heading	pidflo:presence/tuple/status/geopriv/location-info/Dynamic/heading (RFC 5692) [146]
Speed (in KPH/MPH)	pidflo:presence/tuple/status/geopriv10:/location-info/Dynamic/speed
PositionSource	See Table A-12-4 and Table A-12-5
Uncertainty	pidflo:presence/tuple/status/geopriv/location-info/Circle/radius OR pidflo:presence/tuple/status/geopriv/location-info/Sphere/radius uom="urn:ogc:def:uom:EPSG::9001"
Confidence	pidflo:presence/tuple/status/geopriv/location-info/confidence (RFC 7459) [145]
DateStamp Represents the time of the location fix	pidflo:presence/tuple/timestamp Represents the time the PIDF-LO status changed
LocationDescription	If this data field is encountered in the legacy-to-NG9-1-1 mapping, the ensued PIDF-LO would have to have a civic tuple added containing pidflo:presence/tuple/status/geopriv/location-info/civicAddress/LOC
Location Info:Cell Site	
CellID	From SIP P-Access-Network-Info if passed (carrier-specific format)
SectorID	From SIP P-Access-Network-Info if passed (carrier-specific format)
LocationDescription	pidflo:presence/tuple/status/geopriv/location-info/civicAddress/LOC

© Copyright 2011-2022 National Emergency Number Association, Inc.

NENA AQS Element	NG9-1-1 Mapping
Location Info	
Comment	EmergencyCallData.Comment/Comment xml:lang= free text and associated language used
Agencies:Police	From ECRF
Name	LoST:findServiceResponse/mapping/displayName AND LoST:findServiceResponse/mapping/service=urn:emergency:service:responder.police If derivable from the name, append with the appropriate value from the registry (Section 10.6)
TN	LoST:findServiceResponse/mapping/uri=tel: URI with TN expressed as a global number (i.e. starting with +1)
Agencies:Fire	From ECRF
Name	LoST:findServiceResponse/mapping/displayName AND LoST:findServiceResponse/mapping/service=urn:emergency:service:responder.fire If derivable from the name, append with the appropriate value from the registry (Section 10.8)
TN	LoST:findServiceResponse/mapping/uri=tel: URI with TN expressed as a global number (i.e. starting with +1)
Agencies:EMS	From ECRF
Name	LoST:findServiceResponse/mapping/displayName AND LoST:findServiceResponse/mapping/service=urn:emergency:service:responder.ems If derivable from the name, append with the appropriate value from the registry (Section 10.9)
TN	LoST:findServiceResponse/mapping/uri=tel: URI with TN expressed as a global number (i.e. starting with +1)
Agencies: OtherAgencies	From ECRF
Name	LoST:findServiceResponse/mapping/displayName AND LoST:findServiceResponse/mapping/service=urn:emergency:service:responder.“agency” Replace “agency” with appropriate value from the registry (10.5)
TN	LoST:findServiceResponse/mapping/uri=tel: URI with TN expressed as a global number (i.e. starting with +1)
Agencies	
AdditionalInfo	N/A

© Copyright 2011-2022 National Emergency Number Association, Inc.

NENA AQS Element	NG9-1-1 Mapping
ESN	Mapped from PIDF-LO via MCS
SourceInfo: DataProvider	
DataProviderID	EmergencyCallData.ProviderInfo/ProviderID
TN	EmergencyCallData.ProviderInfo/ContactURI in the form of a tel: URI expressed as a global number (i.e. starting with +1)
Name	EmergencyCallData.ProviderInfo/DataProviderString
	Type: EmergencyCallData.ProviderInfo/TypeOfProvider
SourceInfo: AccessProvider	Map when type is EmergencyCallData.ProviderInfo/TypeOfProvider=Access Network Provider
AccessProviderID	EmergencyCallData.ProviderInfo/ProviderID
TN	EmergencyCallData.ProviderInfo/ContactURI in the form of a tel: URI expressed as a global number (i.e. starting with +1)
Name	EmergencyCallData.ProviderInfo/DataProviderString
SourceInfo	
ALIUpdateGMT	N/A
ALIRetrievalGMT	N/A
GeneralUses	Vendor specific mapping
NetworkInfo	
PSAPALIHost	N/A
ResponseALIHost	N/A
PSAPID	N/A
PSAPName	N/A
RouterID	N/A
Exchange	N/A
CLLI	N/A

Table A-12-1 Data Element Mapping

Legacy CoS Code	Legacy Value	NG9-1-1 Data Structure
1	Residence	pidflo:presence/tuple/status/geopriv/method=Manual and EmergencyCallData.ServiceInfo/ServiceType=POTS and EmergencyCallData.ServiceInfo/ServiceEnvironment=Residence and EmergencyCallData.ServiceInfo/ServiceMobility=Fixed

© Copyright 2011-2022 National Emergency Number Association, Inc.

Legacy CoS Code	Legacy Value	NG9-1-1 Data Structure
2	Business	pidflo:presence/tuple/status/geopriv/method=Manual and EmergencyCallData.ServiceInfo/ServiceType=POTS and EmergencyCallData.ServiceInfo/ServiceEnvironment=Business and EmergencyCallData.ServiceInfo/ServiceMobility=Fixed
3	Residence PBX	pidflo:presence/tuple/status/geopriv/method=Manual and EmergencyCallData.ServiceInfo/ServiceType=MLTS-local and EmergencyCallData.ServiceInfo/ServiceEnvironment=Residence and EmergencyCallData.ServiceInfo/ServiceMobility=Fixed
4	Business PBX	pidflo:presence/tuple/status/geopriv/method=Manual and EmergencyCallData.ServiceInfo/ServiceType=MLTS-local and EmergencyCallData.ServiceInfo/ServiceEnvironment=Business and EmergencyCallData.ServiceInfo/ServiceMobility=Fixed
5	Centrex	pidflo:presence/tuple/status/geopriv/method=Manual and EmergencyCallData.ServiceInfo/ServiceType=MLTS-hosted and EmergencyCallData.ServiceInfo/ServiceEnvironment=Business and EmergencyCallData.ServiceInfo/ServiceMobility=Fixed
6	Coin 1 way out	pidflo:presence/tuple/status/geopriv/method=Manual and EmergencyCallData.ServiceInfo/ServiceType=coin;one-way and EmergencyCallData.ServiceInfo/ServiceEnvironment=Business and EmergencyCallData.ServiceInfo/ServiceMobility=Fixed

© Copyright 2011-2022 National Emergency Number Association, Inc.

Legacy CoS Code	Legacy Value	NG9-1-1 Data Structure
7	Coin 2 way	pidflo:presence/ tuple/status/geopriv/method=Manual and EmergencyCallData.ServiceInfo/ServiceType=coin and EmergencyCallData.ServiceInfo/ServiceEnvironment=Business and EmergencyCallData.ServiceInfo/ServiceMobility=Fixed
8	Wireless Phase 0	pidflo:presence/tuple/status/geopriv/method=Manual and EmergencyCallData.ServiceInfo/ServiceType=wireless and EmergencyCallData.ServiceInfo/ServiceMobility =Mobile
9	Residence OPX	pidflo:presence/tuple/status/geopriv/method=Manual and EmergencyCallData.ServiceInfo/ServiceType=POTS;OPX and EmergencyCallData.ServiceInfo/ServiceEnvironment=Residence and EmergencyCallData.ServiceInfo/ServiceMobility=Fixed
0	Business OPX	pidflo:presence/tuple/status/geopriv/method=Manual and EmergencyCallData.ServiceInfo/ServiceType=POTS;OPX and EmergencyCallData.ServiceInfo/ServiceEnvironment=Business and EmergencyCallData.ServiceInfo/ServiceMobility=Fixed
A	Customer owned Coin	pidflo:presence/tuple/status/geopriv/method=Manual and EmergencyCallData.ServiceInfo/ServiceType=Coin and EmergencyCallData.ServiceInfo/ServiceEnvironment=Business and EmergencyCallData.ServiceInfo/ServiceMobility=Fixed
B	Not Available	N/A

© Copyright 2011-2022 National Emergency Number Association, Inc.

Legacy CoS Code	Legacy Value	NG9-1-1 Data Structure
C	VoIP Residence	pidflo:presence/tuple/status/geopriv/method=Manual and EmergencyCallData.ServiceInfo/ServiceType=OTT or digital[83] and EmergencyCallData.ServiceInfo/ServiceEnvironment=Residence and EmergencyCallData.ServiceInfo/ServiceMobility=Unknown[84]
D	VoIP Business	pidflo:presence/tuple/status/geopriv/method=Manual and EmergencyCallData.ServiceInfo/ServiceType=OTT or digital[83] and EmergencyCallData.ServiceInfo/ServiceEnvironment=Business and EmergencyCallData.ServiceInfo/ServiceMobility=Unknown[84]
E	VoIP Coin or Pay Phone	pidflo:presence/tuple/status/geopriv/method=Manual and EmergencyCallData.ServiceInfo/ServiceType=OTT or digital[83];coin and EmergencyCallData.ServiceInfo/ServiceEnvironment=Business and EmergencyCallData.ServiceInfo/ServiceMobility=Unknown[84]
F	VoIP Wireless	pidflo:presence/tuple/status/geopriv/method=Manual and EmergencyCallData.ServiceInfo/ServiceType=OTT or digital[83];wireless and EmergencyCallData.ServiceInfo/ServiceMobility=Mobile
J	VoIP Nomadic	pidflo:presence/tuple/status/geopriv/method=Manual and EmergencyCallData.ServiceInfo/ServiceType=OTT or digital[83] and EmergencyCallData.ServiceInfo/ServiceMobility=Nomadic

[83] If the type of VoIP provider is known, and the VoIP provider is also the Access Infrastructure Provider (AIP) then use "digital", otherwise use "OTT". If the VoIP service is not known, use "digital" for all VoIP types except "J", "VoIP Nomadic".

[84] If the type of service mobility is known, use the correct value, otherwise "Unknown".

© Copyright 2011-2022 National Emergency Number Association, Inc.

Legacy CoS Code	Legacy Value	NG9-1-1 Data Structure
K	VoIP Enterprise	pidflo:presence/tuple/status/geopriv/method=Manual and EmergencyCallData.ServiceInfo/ServiceType=OTT or digital[83] and EmergencyCallData.ServiceInfo/ServiceEnvironment=Business and EmergencyCallData.ServiceInfo/ServiceMobility=Unknown[84]
G	Wireless Phase I	pidflo:presence/tuple/status/geopriv/method=Cell and EmergencyCallData.ServiceInfo/ServiceType=wireless and EmergencyCallData.ServiceInfo/ServiceMobility=Mobile
H	Wireless Phase II	pidflo:presence/tuple/status/geopriv/method= (See Table A-12-4 and Table A-12-5 LTY to i3 Mapping) and EmergencyCallData.ServiceInfo/ServiceType=wireless and EmergencyCallData.ServiceInfo/ServiceMobility=Mobile
I	Wireless Phase II returning Phase I	pidflo:presence/tuple/status/geopriv/method=Cell and EmergencyCallData.ServiceInfo/ServiceType=wireless and EmergencyCallData.ServiceInfo/ServiceMobility=Mobile
V	Voice Over IP	pidflo:presence/tuple/status/geopriv/method=Manual and EmergencyCallData.ServiceInfo/ServiceType=OTT or digital[83] and EmergencyCallData.ServiceInfo/ServiceMobility=Unknown[84]

Table A-12-2 Class of Service Mapping

TYS Codes	TYS Values	NG9-1-1 Data Structure
0	Not FX nor Non-Published	Normal SIP header field use
1	FX in 911 serving area	treat as TYS=0
2	FX outside 911 serving area	treat as TYS=0
3	Non-Published	Privacy Header per RFC 3323 [207]

© Copyright 2011-2022 National Emergency Number Association, Inc.

TYS Codes	TYS Values	NG9-1-1 Data Structure
4	Non-Published FX in 911 serving area	treat as TYS=3
5	Non-Published FX outside 911 serving area	treat as TYS=3
6	Local Ported Number (LNP)	N/A
7	Interim Ported Number	N/A
8	PSALI Published	treat as TYS=0
9	PSALI Non-Published	treat as TYS=3

Table A-12-3 Type of Service Mapping

Clarifications on Table A-12-3: Legacy TYS values map to NG9-1-1 values as shown in the Table. For NG9-1-1 to Legacy TYS mapping, the absence of privacy indication maps to TYS=0 and the use of privacy maps to TYS=3.

Value	Name	PIDF-LO Mapping
0	unknown	Method not included in PIDF-LO
1	networkUnspecified	Method not included in PIDF-LO
2	networkAOA	pidflo:presence/tuple/status/geopriv/method=AOA
3	networkTOA	pidflo:presence/tuple/status/geopriv/method= networkTOA
4	networkTDOA	pidflo:presence/tuple/status/geopriv/method= networkTDOA
5	networkRFFingerprinting	pidflo:presence/tuple/status/geopriv/method= networkRFFingerprinting
6	networkCellSector	pidflo:presence/tuple/status/geopriv/method=Cell
7	networkCellSectorwithTiming	pidflo:presence/tuple/status/geopriv/method=TA
16	handsetUnspecified	Method not included in PIDF-LO
17	handsetGPS	pidflo:presence/tuple/status/geopriv/method=GPS
18	handsetAGPS	pidflo:presence/tuple/status/geopriv/method= Device-Assisted_A-GPS
19	handsetEOTD	pidflo:presence/tuple/status/geopriv/method= Device-Assisted_EOTD
20	handsetAFLT	pidflo:presence/tuple/status/geopriv/method= Handset_AFLT
21	handsetEFLT	pidflo:presence/tuple/status/geopriv/method= Handset_EFLT

© Copyright 2011-2022 National Emergency Number Association, Inc.

Value	Name	PIDF-LO Mapping
22	handsetGNSS	pidflo:presence/tuple/status/geopriv/method=GNSS
23	handsetAGNSS	pidflo:presence/tuple/status/geopriv/method=A-GNSS
24	handsetOTDOA	pidflo:presence/tuple/status/geopriv/method=OTDOA
25	handsetTBS	pidflo:presence/tuple/status/geopriv/method=MBS
26	handsetWi-Fi	pidflo:presence/tuple/status/geopriv/method=Handset_WiFi[85]
27	handsetBluetooth	pidflo:presence/tuple/status/geopriv/method=Handset_BLE[85]
32	hybridUnspecified	Method not included in PIDF-LO
33	hybridAGPS_AFLT	pidflo:presence/tuple/status/geopriv/method=hybridAGPS_AFLT
34	hybridCellSector_AFLT	pidflo:presence/tuple/status/geopriv/method=hybridCellSector_AFLT[85]
35	hybridNetworkTDOA_AOA	pidflo:presence/tuple/status/geopriv/method=hybridTDOA_AOA
36	hybridNetworkTDOA_AGPS	pidflo:presence/tuple/status/geopriv/method=hybridTDOA_AGPS
37	hybridTDOA_AGPS_AOA	pidflo:presence/tuple/status/geopriv/method=hybridTDOA_AGPS_AOA
38	hybridAGPS_OTDOA	pidflo:presence/tuple/status/geopriv/method=hybridTDOA_AGPS
39	hybridAGNSS_OTDOA	pidflo:presence/tuple/status/geopriv/method=hybridTDOA_A-GNSS[85]
40	hybridDeviceBased	pidflo:presence/tuple/status/geopriv/method=DBH
41	hybridAGPS_RFPatternMatch	pidflo:presence/tuple/status/geopriv/method=hybridRFPatternMatch_AGPS[85]
42	hybridAGPS_Wi-Fi	pidflo:presence/tuple/status/geopriv/method=hybridWiFi_AGPS[85]
48	cosUnspecified	Method not included in PIDF-LO
49	cosWRLS	pidflo:presence/tuple/status/geopriv/method=Cell Some local variations exist where phase 0 (Manual) is appropriate

[85] Submit method to IANA Method Token Registry.

© Copyright 2011-2022 National Emergency Number Association, Inc.

Value	Name	PIDF-LO Mapping
50	cosWPH1	pidflo:presence/tuple/status/geopriv/method=Cell
51	cosWPH2	Method not included in PIDF-LO
52	cosTEXT	Method not included in PIDF-LO
53	cosFIXD	Method not included in PIDF-LO
54	cosRESD	Method not included in PIDF-LO
55	cosWCVC	Method not included in PIDF-LO
56	cosWDL1	Method not included in PIDF-LO
57	cosWDL2	Method not included in PIDF-LO

Table A-12-4 LNG Mapping for Position Source – E2 to PIDF-LO

Note on Table A-12-4: Mappings have been added in this version for newly designated position sources as found in the NENA Standard for the Implementation of the Wireless Emergency Service Protocol E2, NENA-STA-018.2 (originally 05-001) [230].

Token	PIDF-LO Mapping
CELL	pidflo:presence/tuple/status/geopriv/method=Cell
OTDOA	pidflo:presence/tuple/status/geopriv/method=OTDOA
GPS	pidflo:presence/tuple/status/geopriv/method=GPS
A-GPS	pidflo:presence/tuple/status/geopriv/method=A-GPS
GNSS	pidflo:presence/tuple/status/geopriv/method=GNSS
A-GNSS	pidflo:presence/tuple/status/geopriv/method=A-GNSS
E-OTD	pidflo:presence/tuple/status/geopriv/method= Device-Assisted_EOTD
U-TDOA	pidflo:presence/tuple/status/geopriv/method=UTDOA
AFLT	pidflo:presence/tuple/status/geopriv/method=Handset_AFLT
EFLT	pidflo:presence/tuple/status/geopriv/method=Handset_EFLT
E-CID	pidflo:presence/tuple/status/geopriv/method=E-CID
UNKNOWN	Method not included in PIDF-LO
OTHER	Method not included in PIDF-LO

Table A-12-5 LNG Mapping for Position Method – MLP to PIDF-LO

© Copyright 2011-2022 National Emergency Number Association, Inc.

Appendix B – SI Provisioning Data Model (Normative)

The model defined in the Appendix represents the data to be incorporated in an XML schema that defines the SI. It may not represent data actually stored in the GIS system but it represents the data that is required by the ECRF, the LVF, the Mapping Data Service (MDS), the Geospatial Conversion Service and the MSAG Conversion Service (MCS) to perform their functions adequately and consistently. This data format is aligned with the NG GIS Data format [184] in that it is possible to convert from the format described in NG GIS to this format, or vice versa, algorithmically, without manual intervention. This format uses "related tables" where data such as the name of a street appears once in a CompleteStreetName table, the StreetSegment table has an index into the CompleteStreetName table and the Centerline table has an index into the StreetSegment table for each road segment.

Attribute names and descriptions are drawn from CLDXF [77] when appropriate. Any difference between the definition of fields other than right/left and similar variances between this model and CLDXF are resolved in favor of the CLDXF definition. When provisioning data for an ECRF and LVF through the SI, a 9-1-1 Authority (or 9-1-1 Authority designee) MUST only include GIS data for their geographic area of responsibility and MUST ensure the data includes coverage for the entire extent of that area.

The "Use M/C/O" column contains the following values:

- "M" = Mandatory, a value MUST be provided.
- "C" = Conditional, a value MUST be provided if the listed condition is met, otherwise optional.
- "O" = Optional, a value MAY be provided.

Since the SI uses XML data structures, elements that are Mandatory have "minoccurs=1", while elements that are Conditional or Optional have "minoccurs=0".

The "Type" column contains the following values:

- A: Represents upper/lower case alphabetic characters only, plus the space character (ASCII decimal code 32.
- N: Represents non-negative integers (whole numbers only).
- AN: Represents upper/lower alphabetic characters plus non-negative integers (i.e., alphanumeric characters)
- P: Printable ASCII characters (decimal codes 32 to 126).
- E: UTF-8 restricted to character sets designated by the 9-1-1 Authority, but not including pictographic characters
- U: Represents characters allowed in a URI (see RFC 3986) [126].
- D: Represents a Date field. Represented as a Timestamp as defined in Section 2.3.

© Copyright 2011-2022 National Emergency Number Association, Inc.

- C: Represents a complex data object.

B.1 Centerlines

ATTRIBUTE NAME	USE M/C/O	TYPE	DATA DESCRIPTION
Discrepancy Agency ID	M	U	Agency that supplies the data, and is the agency that receives a Discrepancy Report (DR) should a discrepancy be discovered.
Data Updated	M	D	Date of the last update, as a Timestamp.
Effective Date	O	D	Date the new information goes into effect, as a Timestamp.
Expiration Date	O	D	Date this feature is no longer effective, as a Timestamp.
Unique ID	M	P	Unique ID for each Road Segment, with domain of agency included. The IDs MUST not be re-used when a road is split or deleted. Example: GHC123@houston.eoc.tx
Country Left	M	A	The name of a country on the left side of where the road is located, represented by its two-letter ISO 3166-1 English country alpha-2 code elements in capital letters as specified in CLDXF or its Canadian equivalent. (country in RFC 5139 [53]) Example: US
Country Right	M	A	The name of a country on the right side of where the road is located, represented by its two-letter ISO 3166-1 English country alpha-2 code elements in capital letters as specified in CLDXF or its Canadian equivalent. (country in RFC 5139 [53]) Example: US
State Left	M	A	The name of a state, province, or equivalent on the left side of where the road is located, as specified in CLDXF or its Canadian equivalent. (A1 in RFC 5139 [53]) Example: TX
State Right	M	A	The name of a state, province, or equivalent on the right side of where the road is located, as specified in CLDXF or its Canadian equivalent. (A1 in RFC 5139 [53]) Example: TX

© Copyright 2011-2022 National Emergency Number Association, Inc.

ATTRIBUTE NAME	USE M/C/O	TYPE	DATA DESCRIPTION
County Left[1]	C	P	The name of county or county-equivalent on the left side of where the road is located, as specified in CLDXF or its Canadian equivalent. Must be provided where is there is a county or county equivalent. (A2 in RFC 5139 [53]) Example: Harris
County Right[1]	C	P	The name of county or county-equivalent on the right side of where the road is located, as specified in CLDXF or its Canadian equivalent. Must be provided where is there is a county or county equivalent. (A2 in RFC 5139 [53]) Example: Harris
AdditionalCodeLeft	C	P	A code that specifies the geographic area on the left side of where the road is located. Used in Canada to hold a Standard Geographical Classification code, which differentiates two municipalities with the same name in a province that does not have counties. MUST be provided if assigned.
AdditionalCodeRight	C	P	A code that specifies the geographic area on the right side of where the road is located. Used in Canada to hold a Standard Geographical Classification code, which differentiates two municipalities with the same name in a province that does not have counties. MUST be provided if assigned.
Incorporated Municipality Left	M	E	The name of the incorporated municipality or other general-purpose local governmental unit (if any) on the left side of where the road is located, as specified in CLDXF or its Canadian equivalent. Populate a name of incorporated municipality if it exists, otherwise enter "Unincorporated". (A3 in RFC 5139 [53]) Example: Chicago

© Copyright 2011-2022 National Emergency Number Association, Inc.

ATTRIBUTE NAME	USE M/C/O	TYPE	DATA DESCRIPTION
Incorporated Municipality Right	M	E	The name of the incorporated municipality or other general-purpose local governmental unit (if any) on the right side of where the road is located, as specified in CLDXF or its Canadian equivalent. Populate a name of incorporated municipality if it exists, otherwise enter "Unincorporated". (A3 in RFC 5139 [53]) Example: Chicago
Unincorporated Community Right	C	E	The name of an unincorporated community, on the right side of where the road is located, as specified in CLDXF or its Canadian equivalent (A4 in RFC 5139 [53]). MUST be provided if Incorporated Municipality Right contains "Unincorporated".
Unincorporated Community Left	C	E	The name of an unincorporated community, on the left side of where the road is located, as specified in CLDXF or its Canadian equivalent. (A4 in RFC 5139 [53]]. MUST be provided if Incorporated Municipality Left contains "Unincorporated".
Neighborhood Community Right	O	E	The name of an unincorporated neighborhood, subdivision, or area, on the right side of where the road is located, as specified in CLDXF or its Canadian equivalent. (A5 in RFC 5139 [53])
Neighborhood Community Left	O	E	The name of an unincorporated neighborhood, subdivision, or area, on the left side of where the road is located, as specified in CLDXF or its Canadian equivalent. (A5 in RFC 5139 [53])
Street Segment	M	C	StreetSegment.
Alias Street Segment	O	C	StreetSegment aliases. MAY occur more than once.
Road Class	M	A	Road classes as specified in MAF/TIGER Feature Classification Codes (MTFCC) Attachment D, Series S. Examples: Primary, Secondary, Local, Ramp, Service, Vehicular Trail, Walkway, Alley, Private, Parking Lot, Trail, Other.

© Copyright 2011-2022 National Emergency Number Association, Inc.

ATTRIBUTE NAME	USE M/C/O	TYPE	DATA DESCRIPTION
One-way	M	A	One-way road classification • B or blank – travel in both directions • FT – One-way from FROM node to TO node (in direction of arc); • TF – One way from TO node to FROM Node (opposite direction of arc)
Speed Limit	O	N	Normal Posted Speed in MPH if country is US or KPH if country is Canada
Speed Limit Unit	C	A	MPH or KPH. MUST be provided if Speed Limit is provided.
Postal Community Name Left	C	A	A city name for the postal code of an address, as determined by the postal authority, on the left side of where the road is located, as specified in CLDXF or its Canadian equivalent. (PCN in RFC 5139 [53]). MUST be populated if a Postal Code is assigned.
Postal Community Name Right	C	A	A city name for the postal code of an address, as determined by the postal authority on the right side of where the road is located, as specified in CLDXF or its Canadian equivalent (PCN in RFC 5139 [53]). MUST be populated if a Postal Code is assigned.
Postal Code Left[2]	C	A	Postal Code, on the left side of where the road is located, as specified in CLDXF or its Canadian equivalent (PC in RFC 5139 [53]). MUST be populated if a Postal Code is assigned. Does not include ZIP+4 code.
Postal Code Right[2]	C	A	Postal Code on the right side of where the road is located, as specified in CLDXF or its Canadian equivalent (PC in RFC 5139 [53]). MUST be populated if a Postal Code is assigned. Does not include ZIP+4 code.
MSAG Left	C	C	Unique ID of corresponding entry associated with the Left side of the street in MSAG table. Provided for E9-1-1 and if needed for transition.

© Copyright 2011-2022 National Emergency Number Association, Inc.

ATTRIBUTE NAME	USE M/C/O	TYPE	DATA DESCRIPTION
MSAG Right	C	C	Unique ID of corresponding entry associated with the Left side of the street in MSAG table. Provided for E9-1-1 and if needed for transition.

B.2 Street/Address Structures

B.2.1 CompleteStreetName

ATTRIBUTE NAME	USE M/C/O	TYPE	DATA DESCRIPTION
Street Name Pre Modifier	O	E	A street pre-modifier as specified in CLDXF or its Canadian equivalent. (PRM in RFC 5139 [53]). Examples: Alternate, Business, Bypass, Extended, Historic, Loop, Old, Private, Public, Spur, etc.
Street Name Pre Directional	O	A	A street name pre-directional as specified in CLDXF or its Canadian equivalent. (PRD in RFC 5139 [53])
Street Name Pre Type	O	E	A street name pre-type as specified in CLDXF or its Canadian equivalent. (STP in RFC 6848 [115])
Street Name Pre Type Separator	O	E	A preposition or prepositional phrase between the Street Name Pre Type and the Street Name as specified in CLDXF or its Canadian equivalent. Example: "of the" in "Boulevard of the Allies".
Street Name	M	E	The street name as specified in CLDXF or its Canadian equivalent. (RD in RFC 5139 [53])
Street Name Post Type	O	E	The street name post type as specified in CLDXF or its Canadian equivalent. (STS in RFC 5139 [53])
Street Name Post Directional	O	A	The street name post directional as specified in CLDXF or its Canadian equivalent. (POD in RFC 5139 [53])

© Copyright 2011-2022 National Emergency Number Association, Inc.

ATTRIBUTE NAME	USE M/C/O	TYPE	DATA DESCRIPTION
Street Name Post Modifier	O	E	The street name post modifier as specified in CLDXF or its Canadian equivalent. (POM in RFC 5139 [53]) Examples: Access, Alternate, Business, Bypass, Connector, Extended, Extension, Loop, Private, Public, Scenic, Spur, Ramp, Underpass, Overpass.

B.2.2 CompleteAddressNumber

ATTRIBUTE NAME	USE M/C/O	TYPE	DATA DESCRIPTION
Address Number Prefix	O	P	The address number prefix as specified in CLDXF or its Canadian equivalent. (HNP in RFC 6848 [115])
Address Number	M	N	The Address Number as specified in CLDXF or its Canadian equivalent. (HNO in RFC 5139 [53])
Address Number Suffix	O	P	The Address Number Suffix as specified in CLDXF or its Canadian equivalent.

B.2.3 StreetSegment

ATTRIBUTE NAME	USE M/C/O	TYPE	DATA DESCRIPTION
Complete Street Name	M	C	CompleteStreetName.
Left Address Number Prefix	O	P	An Address Number Prefix as specified in CLDXF or its Canadian equivalent, applying to all address numbers on the left side of the road in the segment.
Left From Address Number	M	N	The address number (as specified in CLDXF or its Canadian equivalent) on the Left side of the road, which corresponds to the left side of the "FROM Node" of the arc segment. It is quite possible that this address is higher than the left "TO Node". Example: 399

© Copyright 2011-2022 National Emergency Number Association, Inc.

ATTRIBUTE NAME	USE M/C/O	TYPE	DATA DESCRIPTION
Left To Address Number	M	N	The address number (as specified in CLDXF or its Canadian equivalent) on the Left side of the road, which corresponds to the left side of the "TO Node" of the arc segment. It is quite possible that this address is lower than the left "From Address". Example: 199
Parity Left	M	A	A single character code that explicitly defines the allowable addresses on the Left side of the road. Valid values include "O", "E", "B", "Z" for odd, even, both, or zero range, respectively.
Left Address Number Suffix	O	P	An Address Number Suffix, as specified in CLDXF or its Canadian equivalent, applying to all address numbers on the left side of the road in a segment.
Validation Left	O	A	TRUE if any Address Number in the range is valid for the left side of the road. FALSE if Address Number must occur in another layer (e.g., Site/Structure) to be valid. If not present, true is assumed.
Right Address Number Prefix	O	P	Like Left Address Number Prefix, but applying to the right side of the road.
Right From Address Number	M	N	Like Left From Address, but applying to the right side of the road.
Right To Address Number	M	N	Like Left To Address, but applying to the right side of the road.
Parity Right	M	A	Like Parity Left, but applying to the right side of the road.
Right Address Number Suffix	O	P	Like Left Address Number Suffix, but applying to the right side of the road.
Validation Right	O	A	Like Validation Left, but applying to the right side of the road.

B.2.4 CompleteAddress

ATTRIBUTE NAME	USE M/C/O	TYPE	DATA DESCRIPTION
Complete Street Name	M	C	CompleteStreetName.

© Copyright 2011-2022 National Emergency Number Association, Inc.

ATTRIBUTE NAME	USE M/C/O	TYPE	DATA DESCRIPTION
Complete Address Number	C	C	CompleteAddressNumber. If Milepost is provided, Complete Address Number is optional, otherwise it is required.
Milepost	O	P	Milepost as specified in CLDXF or its Canadian equivalent (MP in RFC 6848) [115]

B.3 Site/Structure

ATTRIBUTE NAME	USE M/C/O	TYPE	DATA DESCRIPTION
Discrepancy Agency ID	M	U	Agency that last updated the record – Agency ID, (e.g., the FQDN of the 9-1-1 Authority).
Date Updated	M	D	Date of last update, as a Timestamp.
Effective Date	O	D	Date the new layer information goes into effect, as a Timestamp.
Expiration Date	O	D	Date this feature is no longer effective, as a Timestamp.
Unique_ID	M	P	Unique ID for each record.
Country	M	A	The name of a country represented by its two-letter ISO 3166-1 English country alpha-2 code elements in capital ASCII letters, as specified in CLDXF or its Canadian equivalent. (country in RFC 5139 [53]) Example: US
State	M	A	The 2--character abbreviation of a state, province or equivalent, as specified in CLDXF or its Canadian equivalent. (A1 in RFC 5139 [53]) Example: TX
County	C	P	The name of county or county-equivalent as described in CLDXF or its Canadian equivalent (A2 in RFC 5139 [53]). MUST be provided where there is a county or county equivalent. (A2 in RFC 5139 [53]) Example: Harris

© Copyright 2011-2022 National Emergency Number Association, Inc.

ATTRIBUTE NAME	USE M/C/O	TYPE	DATA DESCRIPTION
AdditionalCode[1]	C	P	A code that specifies the geographic area. Used in Canada to hold a Standard Geographical Classification code, which differentiates two municipalities with the same name in a province that does not have counties. MUST be provided if assigned.
Incorporated Municipality	M	E	The name of the incorporated municipality or other general-purpose local governmental unit as specified in CLDXF or its Canadian equivalent[3]. Populate a name of incorporated municipality if it exists, otherwise enter "Unincorporated" (A3 in RFC 5139 [53]) Example: Chicago
Unincorporated Community	C	E	The name of an unincorporated community, division, or area, as specified in CLDXF or its Canadian equivalent (A4 in RFC 5139 [53]). If Incorporated Municipality contains "Unincorporated", it MUST be provided, otherwise OPTIONAL.
Neighborhood Community	O	E	The name of an unincorporated neighborhood, subdivision, or area, as specified in CLDXF or its Canadian equivalent. (A5 in RFC 5139 [53])
Address	C	C	CompleteAddress. MUST be present unless Complete Landmark Name is populated.
Alias Address	O	C	CompleteAddress aliases. MAY occur more than once.
Postal Community Name	C	A	A city name for the postal code of an address, as determined by the postal authority, as specified in CLDXF or its Canadian equivalent. (PCN in RFC 5139 [53]). MUST be populated if there is an assigned postal code.
Postal Code[2]	C	A	Postal code (PC in RFC 5139 [53]). MUST be populated if there is an assigned postal code. Does not contain the ZIP+4 code. Examples: 05421, G1R 1M9
Postal Code Extension	O	P	Contains the ZIP+4 code or equivalent.

© Copyright 2011-2022 National Emergency Number Association, Inc.

ATTRIBUTE NAME	USE M/C/O	TYPE	DATA DESCRIPTION
Building	O	E	The name of a building as specified in CLDXF or its Canadian equivalent. (BLD in RFC 5139 [53]) Examples: DuPont Hotel, Shiloh Church, Tower B
Floor	O	P	A floor, story, or level within a building as specified in CLDXF or its Canadian equivalent. (FLR in RFC 5139 [53])
Unit	O	P	A group or suite of rooms within a building that are under common ownership or tenancy, typically having a common primary entrance, as specified in CLDXF or its Canadian equivalent. (UNIT in RFC 5139 [53]) Examples: Apartment 101, Suite 233-A
Room	O	P	A single room within a building or unit as specified in CLDXF or its Canadian equivalent. (ROOM in RFC 5139 [53]) Examples: Bedroom, Exam Room 3, Ballroom
Seat	O	P	A place where a person might sit within a room as specified in CLDXF or its Canadian equivalent. (SEAT in RFC 5139 [53]) Examples: Seat 35A, Cubicle 1A213
Complete Landmark Name	O	E	The complete name by which a prominent feature is publicly known as specified in CLDXF or its Canadian equivalent. (LMK in RFC 5139 [53])
Landmark Name Part	C	E	A part of the name by which a prominent feature is publicly known as specified in CLDXF or its Canadian equivalent (LMKP the NENA extension to PIDF-LO). MUST be populated if Complete Street Name is not provided, otherwise OPTIONAL.
Additional Location Information	O	E	A part of a subaddress that is not a building, floor, unit, room, or seat as specified in CLDXF or its Canadian equivalent. (LOC in RFC 5139 [53])

© Copyright 2011-2022 National Emergency Number Association, Inc.

ATTRIBUTE NAME	USE M/C/O	TYPE	DATA DESCRIPTION
Place-Type	O	AN	Type of place as specified in CLDXF or its Canadian equivalent. (PLC in RFC 5139 [53]) Examples: office, store, school, residential
AdditionalDataURI	O	U	URI of Additional Data for this site/structure. MAY occur more than once.
MSAG	C	P	Unique ID of corresponding entry in MSAG table. Provided for E9-1-1 and if needed for transition.
MSAG Street Exception	O	P	Unique ID of corresponding entry in MSAG table

B.4 State Boundary

ATTRIBUTE NAME	USE M/C/O	TYPE	DATA DESCRIPTION
Discrepancy Agency ID	M	U	Agency that last updated the record – Agency ID (e.g., the FQDN of the 9-1-1 Authority).
Date Updated	M	D	Date of the last update, as a Timestamp.
Effective Date	O	D	Date the new layer information goes into effect, as a Timestamp.
Expiration Date	O	D	Date this feature is no longer effective, as a Timestamp.
Unique_ID	M	P	Unique ID for each record.
Country	M	A	The name of a country represented by its two-letter ISO 3166-1 English country alpha-2 code elements in capital ASCII letters, as specified in CLDXF or its Canadian equivalent. (country in RFC 5139 [53]) Example: US
State	M	A	The name of a state, province, or equivalent, as specified in CLDXF or its Canadian equivalent. (A1 in RFC 5139 [53]) Example: TX

© Copyright 2011-2022 National Emergency Number Association, Inc.

B.5 County Boundary

ATTRIBUTE NAME	USE M/C/O	TYPE	DATA DESCRIPTION
Discrepancy Agency ID	M	U	Agency that last updated the record – Agency ID (e.g., the FQDN of the 9-1-1 Authority).
Date Updated	M	D	Date of the last update as a Timestamp.
Effective Date	O	D	Date the new layer information goes into effect, as a Timestamp.
Expiration Date	O	D	Date this feature is no longer effective, as a Timestamp.
Unique_ID	M	P	Unique ID for each record.
Country	M	A	The name of a country represented by its two-letter ISO 3166-1 English country alpha-2 code elements in capital ASCII letters, as specified in CLDXF or its Canadian equivalent. (country in RFC 5139 [53]) Example: US
State	M	A	The name of a state, province, or equivalent, as specified in CLDXF or its Canadian equivalent. (A1 in RFC 5139 [53]) Example: TX
County	M	P	The name of county or county-equivalent as specified in CLDXF or its Canadian equivalent. (A2 in RFC 5139 [53]) Example: Harris

B.6 Incorporated Municipality Boundary

ATTRIBUTE NAME	USE M/C/O	TYPE	DATA DESCRIPTION
Discrepancy Agency ID	M	U	Agency that last updated the record – Agency ID (e.g., the FQDN of the 9-1-1 Authority).
Date Updated	M	D	Date of last update, as a Timestamp.
Effective Date	O	D	Date the new layer information goes into effect, as a Timestamp
Expiration Date	O	D	Date this feature is no longer effective, as a Timestamp.
Unique_ID	M	P	Unique ID for each record.

© Copyright 2011-2022 National Emergency Number Association, Inc.

ATTRIBUTE NAME	USE M/C/O	TYPE	DATA DESCRIPTION
Country	M	A	The name of a country represented by its two-letter ISO 3166-1 English country alpha-2 code elements in capital ASCII letters, as specified in CLDXF or its Canadian equivalent. (country in RFC 5139 [53]) Example: US
State	M	A	The name of a state, province, or equivalent as specified in CLDXF or its Canadian equivalent. (A1 in RFC 5139 [53]) Example: TX
County	C	P	The name of county or county-equivalent as specified in CLDXF or its Canadian equivalent. (A2 in RFC 5139 [53]). MAY be omitted if the boundary straddles more than one county. Example: Harris
AddtionalCode[1]	C	P	A code that specifies the geographic area. Used in Canada to hold a Standard Geographical Classification code, which differentiates two municipalities with the same name in a province that does not have counties. MUST be provided if assigned.
Incorporated Municipality	M	E	The name of the incorporated municipality or other general-purpose local governmental unit as specified in CLDXF or its Canadian equivalent. Populate a name of incorporated municipality if it exists, otherwise enter "Unincorporated". (A3 in RFC 5139 [53]) Example: Chicago

B.7 Unincorporated Community Boundary

ATTRIBUTE NAME	USE M/C/O	TYPE	DATA DESCRIPTION
Discrepancy Agency ID	M	U	Agency that last updated the record – Agency ID (e.g., the FQDN of the 9-1-1 Authority).
Date Updated	M	D	Date of last update, as a Timestamp.

© Copyright 2011-2022 National Emergency Number Association, Inc.

ATTRIBUTE NAME	USE M/C/O	TYPE	DATA DESCRIPTION
Effective Date	O	D	Date the new layer information goes into effect, as a Timestamp.
Expiration Date	O	D	Date this feature is no longer effective, as a Timestamp.
Unique_ID	M	P	Unique ID for each record
Country	M	A	The name of a country represented by its two-letter ISO 3166-1 English country alpha-2 code elements in capital ASCII letters, as specified in CLDXF or its Canadian equivalent. (country in RFC 5139 [53]) Example: US
State	M	A	The name of a state, province or equivalent, as specified in CLDXF or its Canadian equivalent. (A1 in RFC 5139 [53]) Example: TX
County	C	P	The name of county or county-equivalent as specified in CLDXF or its Canadian equivalent. (A2 in RFC 5139 [53]). MAY be omitted if the boundary straddles more than one county. Example: Harris
AdditionalCode[1]	C	P	A code that specifies the geographic area. Used in Canada to hold a Standard Geographical Classification code, which differentiates two municipalities with the same name in a province that does not have counties. MUST be provided if assigned, but MAY be omitted if boundary straddles more than one Additional Code.
Incorporated Municipality	M	E	The name of the incorporated municipality or other general-purpose local governmental unit as specified in CLDXF or its Canadian equivalent. Populate a name of incorporated municipality if it exists, otherwise enter "Unincorporated". (A3 in RFC 5139 [53]) Example: Chicago
Unincorporated Community	M	E	The name of an unincorporated community, as specified in CLDXF or its Canadian equivalent. (A4 in RFC 5139 [53])

© Copyright 2011-2022 National Emergency Number Association, Inc.

B.8 Neighborhood Community Boundary

ATTRIBUTE NAME	USE M/C/O	TYPE	DATA DESCRIPTION
Discrepancy Agency ID	M	U	Agency that last updated the record – Agency ID (e.g., the FQDN of the 9-1-1 Authority).
Date Updated	M	D	Date of the last update as a Timestamp
Effective Date	O	D	Date the new layer information goes into effect, as a Timestamp.
Expiration Date	O	D	Date this feature is no longer effective, as a Timestamp.
Unique_ID	M	P	Unique ID for each record.
Country	M	A	The name of a country represented by its two-letter ISO 3166-1 English country alpha-2 code elements in capital ASCII letters, as specified in CLDXF or its Canadian equivalent. (country in RFC 5139 [53]) Example: US
State	M	A	The name of a state, province, or equivalent, as specified in CLDXF or its Canadian equivalent. (A1 in RFC 5139 [53]) Example: TX
County	C	P	The name of county or county-equivalent as specified in CLDXF or its Canadian equivalent. (A2 in RFC 5139 [53]) MAY be omitted if the boundary straddles more than one county. Example: Harris
AdditionalCode[1]	C	P	A code that specifies the geographic area. Used in Canada to hold a Standard Geographical Classification code, which differentiates two municipalities with the same name in a province that does not have counties. MUST be provided if assigned, but MAY be omitted if boundary straddles more than one Additional Code.

© Copyright 2011-2022 National Emergency Number Association, Inc.

ATTRIBUTE NAME	USE M/C/O	TYPE	DATA DESCRIPTION
Incorporated Municipality	M	E	The name of the incorporated municipality or other general-purpose local governmental unit as specified in CLDXF or its Canadian equivalent. Populate a name of incorporated municipality if it exists, otherwise enter "Unincorporated". (A3 in RFC 5139 [53]) Example: Chicago
Unincorporated Community	O	E	The name of an unincorporated community, as specified in CLDXF or its Canadian equivalent. (A4 in RFC 5139 [53])
Neighborhood Community	M	E	The name of the Neighborhood, as specified in CLDXF or its Canadian equivalent. (A5 in RFC 5139 [53])

B.9 Service Boundary

Most of the Country/State/Municipality fields are optional, since they are not needed, and boundaries may straddle more than one of those fields.

ATTRIBUTE NAME	USE M/C/O	TYPE	DATA DESCRIPTION
Discrepancy Agency ID	M	U	Agency that last updated the record – Agency ID (e.g., the FQDN of the 9-1-1 Authority).
Date Updated	M	D	Date of the last update, as a Timestamp.
Effective Date	O	D	Date the new layer information goes into effect, as a Timestamp.
Expiration Date	O	D	Date this feature is no longer effective, as a Timestamp.
Unique_ID	M	P	Unique ID for each record.
Country	O	A	The name of a country represented by its two-letter ISO 3166-1 English country alpha-2 code elements in capital ASCII letters, as specified in CLDXF or its Canadian equivalent. (country in RFC 5139 [53]) Example: US

© Copyright 2011-2022 National Emergency Number Association, Inc.

ATTRIBUTE NAME	USE M/C/O	TYPE	DATA DESCRIPTION
State	O	A	The name of a state, province, or equivalent, as specified in CLDXF or its Canadian equivalent. (A1 in RFC 5139 [53]) Example: TX
County	O	P	The name of county or county-equivalent as specified in CLDXF or its Canadian equivalent. (A2 in RFC 5139 [53]) Example: Harris
AdditionalCode[1]	O	P	A code that specifies the geographic area. Used in Canada to hold a Standard Geographical Classification code, which differentiates two municipalities with the same name in a province that does not have counties.
Incorporated Municipality	O	E	The name of the incorporated municipality or other general-purpose local governmental unit as specified in CLDXF or its Canadian equivalent. Populate a name of incorporated municipality if it exists, otherwise enter "Unincorporated". (A3 in RFC 5139 [53]) Example: Chicago
Unincorporated Community	O	E	The name of an unincorporated community, as specified in CLDXF or its Canadian equivalent. (A4 in RFC 5139 [53])
Neighborhood Community	O	E	Neighborhood or other informal designation for a part of a community as specified in CLDXF or its Canadian equivalent. (A5 in RFC 5139) [53])
AgencyId	M	U	Unique FQDN for the Service.
ServiceResponse	M	C	Service supplied for this boundary. MAY occur more than once.

B.9.1 Service Response

ATTRIBUTE NAME	USE M/C/O	TYPE	DATA DESCRIPTION
Service URI	M	U	URI for Routing. Example: sip:sos@psap.columbus.oh.us

© Copyright 2011-2022 National Emergency Number Association, Inc.

ATTRIBUTE NAME	USE M/C/O	TYPE	DATA DESCRIPTION
Service URN	M	U	The URN/URL for the Emergency Service or other Well-Known Service (e.g., "urn:service:sos" for a PSAP or "urn:service:sos.ambulance" for an ambulance service). Per RFC 5031 [45]
Service Number	O	P	The emergency services number appropriate for the location provided in the query. "911" is assumed if not provided.
Agency vCard URI	M	U	URI for the vCARD of contact information.
Display Name	M	P	Display Name of the Service. Example: Houston FD

B.10 MSAG

ATTRIBUTE NAME	USE M/C/O	TYPE	DATA DESCRIPTION
Discrepancy Agency ID	M	U	Agency that last updated the record – Agency ID (e.g., the FQDN of the 9-1-1 Authority).
Date Updated	M	D	Date of the last update, as a Timestamp.
Effective Date	O	D	Date the new layer information goes into effect, as a Timestamp.
Expiration Date	O	D	Date this feature is no longer effective, as a Timestamp.
Unique_ID	M	P	Unique ID for each record.
Prefix Directional	O	P	Leading street direction prefix.
Street Name	M	E	Street Name.
Street Suffix	O	E	Street Type.
Post Directional	O	P	Trailing street direction suffix.
MSAG Community Name	M	P	Service community name.
County ID	O	P	County Identifier.
AdditionalCode[1]	C	P	A code that specifies the geographic area. Used in Canada to hold a Standard Geographical Classification code, which differentiates two municipalities with the same name in a province that does not have counties. MUST be provided if assigned.
State/Province	M	P	State or Province.

© Copyright 2011-2022 National Emergency Number Association, Inc.

ATTRIBUTE NAME	USE M/C/O	TYPE	DATA DESCRIPTION
ESN	C	N	Emergency Service Number, MUST be provided if any LPGs or egress LSRGs exist in the ESInet or other legacy systems that require an ESN remain.

B.10.1 MSAG Street Number Exception

ATTRIBUTE NAME	USE M/C/O	TYPE	DATA DESCRIPTION
Discrepancy Agency ID	M	U	Agency that last updated the record – Agency ID (e.g., the FQDN of the 9-1-1 Authority).
Date Updated	M	D	Date of last update, as a Timestamp.
Effective Date	O	D	Date the new layer information goes into effect, as a Timestamp.
Expiration Date	O	D	Date this feature is no longer effective, as a Timestamp.
Unique_ID	M	P	Unique ID for each record.
Street Number	M	P	Street Number as found in MSAG.
Street Number Suffix	O	P	Street Number Suffix as found in MSAG.
ESN	O	P	Emergency Service Number associated with this House Number, Street Name, and Community Name.

[1] In Canada, there may not be counties in some areas, but in a given province, there can be two municipalities with the same name. Where there is no county, and there is name collision in the Municipality or MSAG Community name, a code may be placed in this field to differentiate the instances.

[2] The USPS considers ZIP codes to be delivery points instead of areas. There may be differences between this depiction and actual ZIP code mailing address.

[3] Used in legacy systems and in transition. Not used in a full i3 implementation.

© Copyright 2011-2022 National Emergency Number Association, Inc.

Appendix C – Support for PSAP Call Control Features (Normative)

PSAP Call Control Features allow a Public Safety Answering Point (PSAP) to prevent a call from being taken down when an emergency caller attempts to disconnect, and also allow the PSAP attendant, after being signaled that the caller attempted to disconnect, to invite an emergency caller to rejoin a conversation by providing alerting to the caller. These features are currently offered as part of emergency services deployments in North America and around the world, and some jurisdictions even mandate the availability of some of these features.

While support of PSAP Call Control Features is not a required component of all i3 implementations, this Appendix describes the procedures necessary to support PSAP Call Control Features in those networks in which such capabilities are desired or required. This appendix assumes that PSAPs and originating networks know when they are operating in an environment in which PSAP Call Control Features are supported. The set of features that are referred to collectively as PSAP Call Control. Features consist of: Called Party Hold (CPH)[86], Enhanced Called Party Hold (ECPH), Switch-hook Status, and on/off-hook Ringback.

Functional Elements defined in this document that are involved in emergency calls supporting PSAP Call Control Features MUST comply with the requirements set forth in this Appendix. This includes MANDATORY support of the SDP "a" attribute values "suspended" and media feature tag "urn:emergency:media-feature.psap-call-control" for Functional Elements on the call path and processing SDP in call scenarios in which these are used.

C.1 Assumptions Regarding Behavior in the Originating Network

This document does not place any specific requirements on originating networks, however the procedures in this Appendix are based on a set of assumptions regarding the signaling generated by a legacy or SIP-based originating network toward an i3 ESInet/NGCS in support of PSAP Call Control Features. The text in this section describes these assumptions so that the reader will better understand the procedures associated with i3 Functional Elements and PSAPs that are normatively described in subsequent sections of this Appendix.

[86] Also referred as "Calling Party Hold", "Bureau Hold", "Network Hold", "Connection Hold", "Originator Hold", "Caller Hold", "Emergency Calling Service Call Hold", and "Forced Hold".

© Copyright 2011-2022 National Emergency Number Association, Inc.

C.1.1 Assumed Behavior in a Legacy Originating Network

C.1.1.1 SS7 Signaling from Originating End Office

If Called Party Hold/Switch-hook Status is supported in a legacy originating network that uses outgoing SS7-supported trunks from the originating end office for emergency calls, it is assumed that the originating network will signal the availability of the Called Party Hold feature by generating an SS7 Initial Address Message (IAM) that contains a Service Activation Parameter (SAP) with a Feature Code Indicator (FCI) set to "hold available", as described in ATIS-1000628.a.2001(2010) [136] and ATI_-1000666.1999 (2014) [91]. If connection hold is desired/required for the call, the originating network expects to receive a SAP parameter with an FCI set to "hold request" in an SS7 Address Complete Message (ACM) (or SS7 Facility [FAC] message if an ACM has already been received for that circuit). If Called Party Hold is active for an emergency call, and the emergency caller attempts to disconnect from the call, the legacy originating switch will generate an SS7 FAC message that contains a SAP with an FCI indicating "disconnect request". In response to this FAC message, the legacy originating switch will either receive periodic SS7 FAC messages that contain a SAP with an FCI set to "hold continuation request" (if the PSAP wishes to maintain the existing connection) or an SS7 Release (REL) message (if the PSAP wishes to release the connection).

If the emergency caller goes off-hook after the "disconnect request" has been sent, and an SS7 REL has not yet been received, the legacy originating switch will generate an SS7 FAC message that contains a SAP with an FCI indicating "reconnect request".

The procedures described above are also expected from originating networks supporting Enhanced Called Party Hold. Note that Enhanced Called Party Hold requires the addition of an ECPH timer[87] downstream from the originating network. When the ECPH timer expires prior to the call being answered at the PSAP, the legacy originating switch may receive an SS7 FAC message containing a SAP with an FCI indicating "hold release request".

When the Ringback feature is invoked by the PSAP attendant on a held connection in an originating network that supports PSAP Call Control features and call delivery via SS7-controlled trunk groups, it is expected that the originating network will be capable of receiving and processing an SS7 FAC message that contains an FCI indicating "Ringback request" and will apply the appropriate treatment towards the caller depending on the call state (ringing for on-hook, or Receiver-Off-Hook [ROH], also known as "howler" tone, for

[87] The ECPH timer controls the time ECPH is active for a given 9-1-1 call. In legacy implementations, it is a configurable parameter typically set in the range of a few tens of seconds to a few minutes after call initiation.

© Copyright 2011-2022 National Emergency Number Association, Inc.

off-hook). In this scenario, the originating network is expected to supply audible ringing back towards the PSAP.

C.1.1.2 MF Signaling from Originating End Office

If Called Party Hold/Switch-hook Status is supported in a legacy originating network that uses outgoing MF trunk groups from the originating end office for emergency calls, then upon receiving an off-hook signal from the caller followed by the digits "911", the end office will seize an outgoing trunk to a Legacy Network Gateway (LNG). When the originating end office receives a wink back from the LNG, the end office will outpulse the called number (i.e., KP + 911 + ST), and will wait for an ANI request signal. Upon receiving the ANI request signal, the end office will outpulse the ANI sequence using CAMA (I + 7-digit ANI) or Feature Group D operator-type (II + 7/10-digit ANI) MF signaling. While the PSAP is being alerted, audible ringing will be delivered to the caller. When the PSAP answers the call, an answer ("off-hook") signal will be delivered to the originating end office.

If an emergency caller subsequently goes on-hook, an on-hook signal will be sent forward by the originating switch. Feature-specific processing of the MF signals generated by the end office will be applied by downstream elements based on trunk group provisioning. Since Called Party Hold/Switch-hook Status is supported by the legacy originating switch, the connection to the LNG is expected to be maintained.

If the caller subsequently goes off-hook, an off-hook signal will be sent forward, and the behavior of downstream elements will be determined based on provisioning associated with the outgoing MF trunk group.

If the Ringback feature is invoked by the PSAP attendant on a held connection in an originating network that supports MF trunking out of the end office, it is expected that the originating network will pass the appropriate treatment, as applied by the downstream element (in this case the LNG), through towards the caller as follows: If an off-hook Ringback is invoked by a PSAP attendant on an established connection, the originating network is expected to pass the appropriate treatment (e.g., ROH/howler tone), as applied by the LNG, through to the caller. If the on-hook Ringback feature is invoked by the PSAP attendant on a held connection to an LNG associated with an emergency call that was delivered via an MF trunk group out of the end office, it is expected that normal ringing will be used to alert the caller to the Ringback attempt. As described in Section C.4.4.2, the PIF component of the LNG will also return a SIP 180 Ringing message to the NIF component in response to an incoming re-INVITE message containing an Alert-Info header field from the NIF component. Note that neither the originating network nor the LNG will provide audible ringing toward the PSAP in this case.

© Copyright 2011-2022 National Emergency Number Association, Inc.

C.1.2 Assumed Behavior in a SIP-Based Originating Network

If a SIP-based originating network is operating in a jurisdiction in which Called Party Hold/Switch-hook Status is supported, this Appendix assumes that the SIP-based originating network will behave in one of the following ways:

1. The SIP-based originating network follows the procedures defined in PKT-SP-RSTF-C01-140314 [137] and PKT-SP-CMSS1.5-I07-120412 [138]. According to Section 8.5.5.8 of PKT-SP-RSTF-C01-140314 [137], because only the PSAP knows if the network hold feature is in effect, the originating network must assume that network hold could be applied. Therefore the originating network processing of a disconnect request from the calling user will be different from normal disconnect processing if it occurs after the PSAP has answered the call. Specifically, upon receiving a disconnect request from the caller after the PSAP has answered the call, the originating network is expected to send a SIP re-INVITE containing an associated SDP with attribute "a= inactive" and a Priority header field set to "emergency", and set a Network Hold timer[88]. If the user subsequently attempts to reconnect to the call, the originating network is expected to send a re-INVITE with an updated SDP offer and stop the Network Hold timer. If the originating network receives 200 OK responses to the re-INVITE messages, it will interpret these as indications of acceptance of the associated media offers.

   If the originating network supports Enhanced Called Party Hold, it is expected to set an ECPH timer at call setup time. Upon receiving a disconnect request from the caller before the PSAP has answered the call, the originating network will send a SIP UPDATE with an associated SDP "a" attribute set to "inactive" and a Priority header field set to "emergency". If the user subsequently attempts to reconnect to the call prior to a PSAP answer, the originating network is expected to send an UPDATE with an updated SDP offer. If the originating network receives 200 OK responses to the UPDATE messages, it will interpret these as indications of acceptance of the associated media offers. If the originating network receives the 200 OK response to the original INVITE, it will cancel the ECPH timer, if not expired. The originating network is expected to process received SIP BYE messages as specified in RFC 3261. If the Network Hold timer expires before the user attempts to reconnect to the call, the originating network is expected to generate a SIP BYE message. Additionally, if the ECPH timer expires before the call is answered by the PSAP attendant, the originating network is expected to generate a SIP CANCEL message.

[88] See Table 54 of RFC 3398 [139] for guidance on the Network Hold timer value.

© Copyright 2011-2022 National Emergency Number Association, Inc.

If the originating network receives a re-INVITE message that contains an Alert-Info header field (i.e., as a result of a Ringback request being initiated by the PSAP), the originating network is expected to apply the associated Ringback alerting treatment (i.e., regular ringing or receiver off-hook/howler tone, as identified in the ringing tone URI included in the Alert-Info header field) to the emergency caller. The originating network is also expected to return a SIP 180 Ringing message to/toward the i3 PSAP or Legacy PSAP Gateway (LPG). Note that the originating network should not provide audible ring to the PSAP.

2. Alternatively, the SIP-based originating network may follow the procedures defined between the LNG-NIF and the NGCS in Sections C.3.1.1.2, C.3.1.2.2, C.4.4.1 and C.5.2.2. Additionally, because such originating networks may support nomadic devices, additional procedures are required to confirm whether the features can be supported end-to-end. This is accomplished by including the media feature tag "urn:emergency:media-feature.psap-call-control" in a Contact header field of the original SIP INVITE and any subsequent requests in-dialog. A PSAP or LPG supporting PSAP Call Control features will include the same media feature tag value in all responses within the dialog. If both parties have received the media feature tag, they must assume that PSAP Call Control features are in effect. From this point, the originating network processing of a disconnect request from the calling user will be different from normal disconnect processing if it occurs after the PSAP has answered the call. Specifically, upon receiving a disconnect request from the caller after the PSAP has answered the call, the originating network is expected to send a SIP re-INVITE containing an associated SDP with attribute "a=suspended" and set a Network Hold timer. If the user subsequently attempts to reconnect to the call, the originating network is expected to send a re-INVITE with an updated SDP offer with attribute "a=sendrecv" and stop the Network Hold timer. If the originating network receives 200 OK responses to the re-INVITE messages, it will interpret these as indications of acceptance of the associated media offers.

   If the originating network supports Enhanced Called Party Hold, it is expected to set an ECPH timer at call setup time. Upon receiving a disconnect request from the caller before the PSAP has answered the call, the originating network will send a SIP UPDATE with an associated SDP with attribute "a=suspended". If the disconnect occurs before the response to the original INVITE is received and if that response does not contain the media feature tag "urn:emergency:media-feature.psap-call-control", the originating network is expected to immediately send a SIP CANCEL and cancel the ECPH timer. If the disconnect occurs after a response to the original INVITE containing the media feature tag is received and the user subsequently attempts to reconnect to the call prior to PSAP answer, the originating network is expected to send an UPDATE with an updated SDP offer with attribute

© Copyright 2011-2022 National Emergency Number Association, Inc.

"a=sendrecv". If the originating network receives 200 OK responses to the initial INVITE and subsequent UPDATE messages, it will interpret these as indications of acceptance of the associated media offers and cancel the ECPH timer.

The originating network is expected to process received SIP BYE messages as specified in RFC 3261. If the Network Hold timer expires before the user attempts to reconnect to the call, the originating network is expected to generate a SIP BYE message. Additionally, if the ECPH timer expires before the call is answered by the PSAP attendant, the originating network is expected to generate a SIP CANCEL message.

If the originating network receives a re-INVITE message that contains an Alert-Info header field (i.e., as a result of a Ringback request being initiated by the PSAP), the originating network is expected to apply the associated Ringback alerting treatment (i.e., regular ringing or receiver off-hook/howler tone, as identified in the ringing tone URI included in the Alert-Info header field) to the emergency caller. If Ringback is signaled through the "P-DCS-OSPS:RING" header field[89], the originating network is expected to apply the appropriate Ringback alerting treatment based on its knowledge of the hook state of the calling device. The originating network is also expected to return a SIP 180 Ringing message to/toward the i3 PSAP or LPG. Note that the originating network should not provide audible ringing to the PSAP.

3. The originating network does not support any Called Party Hold/Enhanced Called Party Hold/Switch-hook Status-specific call handling procedures. If a disconnect request is received from the caller, the UA generates a SIP BYE message (or SIP CANCEL if the 200 OK response has not been received), as specified in RFC 3261. It is expected to follow the procedures specified in RFC 6881 [46] for handling emergency call originations.

C.2 Bridging Considerations

A conference bridge in an i3 ESInet that supports the functionality described in Section 4.7 (referred to in this Appendix as the "Bridge") MUST be aware of the status of PSAP Call Control support of all parties involved in a conference. The following sub-sections define the procedures required depending on the Bridging method implemented.

If only the caller supports PSAP Call Control features and the PSAPs on the conference do not, the Bridge, upon receiving a switch-hook status change from the caller, MUST send a BYE message to the caller. The Bridge MUST also send a NOTIFY message to the

[89] See Section C.4.1 for further details.

© Copyright 2011-2022 National Emergency Number Association, Inc.

subscribers to the conference noting the conference status of the caller by setting the <endpoint> element with a <status> sub-element set to "disconnected" and a <disconnection-method> sub-element set to "booted", as per RFC 4575 [40].

C.2.1 SIP Ad Hoc Method

A Bridge that uses the "SIP Ad Hoc" method must be informed of the support of PSAP Call Control features by the conference participants. When invoking the Bridge, a Transfer-from PSAP supporting PSAP Call Control features MUST signal in the INVITE message (and any subsequent requests in-dialog) to the Bridge that it supports PSAP Call Control features by adding the media feature tag "urn:emergency:media-feature.psap-call-control" as part of a Contact header field value of the INVITE message. When adding the caller, the Bridge MUST add the media feature tag "urn:emergency:media-feature.psap-call-control" in the Contact header field of the INVITE message with Replaces. If the Caller supports PSAP Call Control Features, the Caller (or B2BUA[90]) MUST add the media feature tag "urn:emergency:media-feature.psap-call-control" in all responses, provisional or final, to the INVITE and any subsequent requests in-dialog. When adding the Transfer-To PSAP, the Bridge MUST add the media feature tag "urn:emergency:media-feature.psap-call-control" in a Contact header field of the outgoing INVITE message, if the caller supports PSAP Call Control features. If it supports PSAP Call Control features, the Transfer-To PSAP MUST add the media feature tag "urn:emergency:media-feature.psap-call-control" in all responses, provisional or final, to the INVITE and any subsequent requests in-dialog. At this point, the Bridge and all parties participating on the conference are aware of PSAP Call Control support.

C.2.2 Route All Calls via a Conference-Aware UA Method

A Bridge that uses the "Route All Calls via a Conference-Aware UA" method MUST maintain state of PSAP Call Control features support, as learned through the signaling of the initial emergency call. If the calling device supports PSAP Call Control features, the Bridge MUST also learn support of PSAP Call Control features of any party added to the conference. The Bridge does so by adding the media feature tag "urn:emergency:media-feature.psap-call-control" as part of a Contact header field value of the INVITE messages (and any subsequent requests in-dialog) sent to parties by the Conference-Aware UA. Parties supporting PSAP Call Control features MUST add the media feature tag "urn:emergency:media-feature.psap-call-control" as part of a Contact header field value of

[90] A B2BUA which supports origination devices/services that do not support Replaces but do support Call Control Features will need to add the media feature tag on the response to INVITE/Replaces. How this is recognized is an implementation detail.

© Copyright 2011-2022 National Emergency Number Association, Inc.

all responses, provisional or final, to the INVITE message and any subsequent requests in-dialog.

C.3 Called Party Hold/Switch-Hook Status

C.3.1 Procedures at the Legacy Network Gateway

C.3.1.1 SS7 Signaling from Originating End Office

When a legacy originating switch receives an emergency call origination and determines that the Called Party Hold feature may be requested by an emergency services network, and the originating switch can support the Called Party Hold feature for the outgoing circuit, the SS7 Initial Address Message (IAM) delivered by the originating switch to the LNG MAY contain a Feature Code Indicator in the Service Activation Parameter (SAP) set to "hold available".

C.3.1.1.1 Procedures at the LNG-PIF Component

Upon receiving an IAM with a SAP, the PIF component of the LNG SHALL follow the procedures in Section 6.1.1.2.2 and 6.1.1.5, with the following modifications. If the PIF component receives an IAM that contains a SAP, it SHALL encapsulate the IAM in the INVITE sent to the NIF component, including the encapsulated message in the body of the INVITE following the procedures specified in Section 5.4.1.2 of ATIS-1000679.2015 [130].

In addition, the PIF component SHALL be capable of receiving a 180 Ringing message from the NIF component that includes an encapsulated ACM message that contains a SAP parameter with a Feature Code Indicator set to "hold request" in the body. The PIF component SHALL generate an ACM, based on the received 180 Ringing message, and SHALL include a SAP parameter with Feature Code Indicator set to "hold request" in the outgoing ACM.

The PIF component SHALL also be capable of receiving a 183 Session Progress message from the NIF component that includes an encapsulated ACM message that contains a SAP parameter with a Feature Code Indicator set to "hold request" in the body. The PIF component SHALL generate an ACM, based on the received 183 Session Progress message, and SHALL include a SAP parameter with Feature Code Indicator set to "hold request" in the outgoing ACM.

If the PIF component subsequently receives an SS7 Facility (FAC) message associated with the incoming SS7-supported trunk group over which the emergency call origination was received, it SHALL encapsulate the FAC message in a SIP INFO (RFC 6086) [149] message, as described in Section 5.4.3 of ATIS-1000679.2015 [130] and send it to the NIF component. This may occur if an emergency call has been established, Called Party Hold is

© Copyright 2011-2022 National Emergency Number Association, Inc.

active on that call, and the switch-hook status of the emergency caller changes. If the emergency caller attempts to disconnect from the call (i.e., goes "on-hook"), the FAC message MUST contain a Feature Code Indicator in the SAP set to "disconnect request". If the emergency caller subsequently goes "off-hook", the PIF component SHALL receive an FAC that contains a Feature Code Indicator in the SAP set to "reconnect request".

If the PIF component receives a SIP INFO containing an encapsulated FAC message from the NIF component, the PIF component SHALL generate an SS7 FAC message based on the encapsulated FAC message.

If, at any time, the PIF component receives a SIP BYE message from NIF component, the PIF component SHALL process that SIP BYE message as described in Section 6.1.1.5. If, at any time, the PIF component receives an SS7 REL message from the legacy originating network, the PIF component SHALL generate a SIP BYE message and send it to the NIF component, as described in Section 6.1.1.2.2.

C.3.1.1.2 Procedures at the LNG-NIF Component

Upon receipt of an INVITE message from the PIF component containing an encapsulated IAM, the NIF component SHALL follow the procedures in Sections 6.1.2.1, 6.1.2.1.1, and 6.1.2.2 with the following modifications. If, based on receipt of a media feature tag with the value "urn:emergency:media-feature.psap-call-control", the NIF component determines that the destination to which the call was delivered supports PSAP Call Control Features, then upon receipt of a 180 Ringing message from the NGCS (that does not contain an encapsulated ACM), the NIF component SHALL generate and send a 180 Ringing message to the PIF component with an encapsulated ACM in the body of that message. If, based on receipt of the media feature tag "urn:emergency:media-feature.psap-call-control", the NIF component determines that the destination to which the call was delivered supports PSAP Call Control Features and the NIF component receives a 183 Session Progress message from the NGCS (that does not contain an encapsulated ACM), the NIF component SHALL generate and send a 183 Session Progress message to the PIF component with an encapsulated ACM in the body of that message. In either case, the NIF component SHALL populate the encapsulated ACM following the procedures described in Section 6.1.1.5 and SHALL also include a SAP with a Feature Code Indicator set to "hold request" in the encapsulated ACM message.

If the NIF component receives a 180 Ringing or 183 Session Progress message that contains an encapsulated ACM, the NIF component SHALL follow the procedures in Section 7.2.1 or 7.2.2, respectively, of ATIS-1000679.2015 [130] for sending a 180 Ringing or 183 Session Progress message to the PIF component.

© Copyright 2011-2022 National Emergency Number Association, Inc.

If the NIF component receives a SIP INFO message from the PIF component, associated with the same emergency call that contains an encapsulated FAC message with the Feature Code Indicator in the SAP set to "disconnect request," the NIF component SHALL generate a re-INVITE message that contains an SDP offer with an "a= suspended" attribute[91]. The re-INVITE message MUST reference the existing dialog so that the i3 PSAP (or LPG, in the case of a legacy PSAP) knows that it is to modify an existing session instead of establishing a new session. The re-INVITE message SHALL include the following information:

- A Request-URI that contains the information provided in the Contact header field of the 200 OK message that was returned in response to the original INVITE message;
- A To header field that contains the same information as the original INVITE message (i.e., the digits "911");
- A From header field that contains the same information as in the original INVITE message;
- A Via header field that is populated with the Element Identifier (see Section 2.1.3) for the LPG;
- A Route header field that contains the same information as in the original INVITE (i.e., the ESRP URI obtained from the ECRF, which should be augmented with the "lr" parameter to avoid Request-URI rewriting);
- A Contact header field that contains the same information as in the original INVITE message (i.e., a SIP URI associated with the LNG), including the media feature tag;
- An SDP with an "a = suspended" attribute to identify that this is related to PSAP Call Control Features.

Upon receiving a 200 OK message from the i3 PSAP/LPG (via the NGCS), indicating that it accepts the change, the NIF component SHALL respond to the 200 OK by returning an ACK message toward the i3 PSAP/LPG. The NIF component SHALL also send a SIP INFO message to the PIF component that contains an encapsulated FAC message with the Feature Code Indicator in the SAP set to "hold continuation request" and will repeat this periodically (e.g., every minute or so) to maintain the connection in the legacy originating network.

[91] Note that the use of a re-INVITE that contains an SDP offer indicating that the originator of the re-INVITE no longer wishes to receive media is consistent with the procedures described in Section 9.2 of IETF RFC 3398 [139]. The use of an "a=" attribute value of "suspended" in the SDP will allow the entity receiving the re-INVITE to associate the message with a disconnect request issued by an emergency caller that is subject to PSAP Call Control features.

© Copyright 2011-2022 National Emergency Number Association, Inc.

If the NIF component receives a SIP INFO message from the PIF component, associated with the same emergency call, that contains an encapsulated FAC message with the Feature Code Indicator in the SAP set to "reconnect request", the NIF component SHALL generate a re-INVITE message with a new SDP offer that contains an attribute of "a=sendrecv". The re-INVITE SHALL contain the same information listed above, except that the SDP will contain the new offer.

Upon receiving a 200 OK message from the i3 PSAP/LPG indicating that it accepts the change, the NIF component SHALL respond to the 200 OK by returning an ACK message toward the i3 PSAP/LPG to acknowledge receipt of the SIP 200 response and to confirm the media has been reactivated.

C.3.1.2 MF Signaling from Originating End Office

C.3.1.2.1 Procedures at the LNG-PIF Component

Upon receiving a trunk seizure (off-hook) from the originating end office, the PIF component of the LNG SHALL return a wink back to the end office. After receiving the called number sequence (i.e., KP + 911 + ST), the PIF component SHALL generate an ANI request signal and await the ANI sequence. If CAMA-type signaling is used on the MF trunk from the originating end office to the LNG, the PIF component of the LNG SHALL be capable of receiving and processing an ANI sequence that consists of "I + 7-digit ANI". If Feature Group D operator-type signaling is used on the MF trunk from the legacy end office to the PIF component of the LNG, the PIF component SHALL be capable of receiving and processing an ANI sequence consisting of "II + 7/10-digit ANI".

The PIF component SHALL follow the procedures in Section 6.1.1.5 for generating a SIP INVITE message and sending it to the NIF component of the LNG.

Also, as described in Section 6.1.1.5, the PIF component of the LNG SHALL be capable of receiving and processing a SIP 100 Trying message passed to it by the NIF component, acknowledging receipt of the INVITE that was previously generated by the PIF component.

The PIF component of the LNG SHALL also be capable of receiving and processing a 180 Ringing message and a 183 Session Progress message from the NIF component. Upon receiving a 180 Ringing message, the PIF component MUST apply audible ringing tone to the calling party.

The PIF component of the LNG SHALL be capable of receiving and processing a 200 OK message, indicating that the call has been answered. Upon receiving the 200 OK message, the PIF SHALL generate an answer signal to the originating end office.

If the PIF component receives an "on-hook" indication from the originating end office switch associated with an existing emergency call delivered over an MF trunk group, the

© Copyright 2011-2022 National Emergency Number Association, Inc.

PIF component SHALL use trunk group provisioning to determine its subsequent behavior. If the provisioning associated with the incoming MF trunk group indicates that Called Party Hold/Switch-hook Status is supported, the PIF component SHALL pass the on-hook/"unseize circuit" telephony event to the NIF component using the mechanisms defined in RFC 5244 [140] (or equivalent), and SHALL maintain the connection to the originating end office switch. If the emergency caller subsequently goes "off-hook", the PIF component SHALL pass the off-hook/"seizure" telephony event to the NIF component using the mechanisms defined in RFC 5244 [140] (or equivalent).

If the provisioning associated with the incoming MF trunk group indicates that Called Party Hold/Switch-hook Status is not supported, and an on-hook signal is received from the originating end office associated with an existing emergency call delivered over an MF trunk group, the PIF component SHALL generate a SIP BYE message and send it to the NIF component, as described in Section 6.1.1.1.

If, at any time, the PIF component receives a SIP BYE message from the NIF component, the PIF component SHALL process that SIP BYE message, return a 200 OK message to the NIF component, acknowledging receipt of the SIP BYE message, as described in Section 6.1.1.5, and SHALL generate an on-hook signal toward the originating switch.

C.3.1.2.2 Procedures at the LNG-NIF Component

Upon receipt of an INVITE message from the PIF component, the NIF component SHALL follow the procedures in Sections 6.1.2.1, 6.1.2.1.1, and 6.1.2.2 for processing that INVITE message and sending an INVITE to the NGCS. Based on provisioning associated with the incoming trunk group parameters in the Contact header field of the INVITE message received from the PIF component, the NIF component SHALL determine whether PSAP Call Control Features are supported for this emergency call.

As described in Section 6.1.2.2, the NIF component SHALL return a SIP 100 Trying message to the PIF after sending the SIP INVITE to the NGCS. The NIF component SHALL also be capable of receiving and processing a 180 Ringing or 183 Session Progress message from the NGCS in response to the SIP INVITE. The NIF component SHALL forward the 180 Ringing or 183 Session Progress message to the PIF component. In addition, the NIF component SHALL determine whether the destination to which the call was delivered supports PSAP Call Control Features based on the presence or absence of the "urn:emergency:media-feature.psap-call-control" media feature tag in a Contact header field of the received 180 Ringing or 183 Session Progress message.

The NIF component SHALL also be capable of receiving and processing a 200 OK message from the NGCS. If the NIF component receives a 200 OK message from the NGCS, it SHALL send it to the PIF component. The NIF component SHALL be capable of receiving and

© Copyright 2011-2022 National Emergency Number Association, Inc.

processing an ACK message from the PIF component in response to the 200 OK message. The NIF component SHALL subsequently send an ACK message to the NGCS.

If the NIF component subsequently receives an on-hook/"unseize circuit" event indication (encoded using RFC 5244 [140] mechanisms or equivalent) from the PIF component associated with the same emergency call (received over an MF trunk group that is provisioned to indicate support for Called Party Hold/Switch-hook Status), and the destination to which the call was delivered also supports PSAP Call Control Features, the NIF component SHALL generate a re-INVITE message with SDP that contains an "a= suspended" attribute, as specified in Section C.3.1.1.2, and forward the re-INVITE to the NGCS.

If, subsequent to receiving an on-hook/unseize circuit event indication, the NIF component receives an off-hook/seize event indication (encoded using RFC 5244 [140] mechanisms or equivalent) from the PIF component associated with the same emergency call, and the destination to which the call was delivered also supports PSAP Call Control Features, the NIF component SHALL generate a re-INVITE message with a new SDP offer with an attribute of "a=sendrecv". As in Section C.3.1.1.2, the re-INVITE will contain the same information as the previous re-INVITE, except that the SDP will contain the new offer.

In both cases, upon receiving a 200 OK message from the i3 PSAP/LPG (via the NGCS) indicating that it accepts the change, the NIF component MUST respond to the 200 OK by returning an ACK message toward the i3 PSAP/LPG confirming the media has been changed.

If the NIF component receives an on-hook/unseize circuit event indication (encoded using RFC 5244 [140] mechanisms or equivalent) from the PIF component associated with an emergency call that was received over an MF trunk group that is provisioned to indicate support for Called Party Hold/Switch-hook Status, and the destination to which the call was delivered does not support PSAP Call Control Features, the NIF component SHALL send a BYE message to the NGCS and a BYE message to the PIF component.

If, at any time, the NIF component receives a SIP BYE message from the NGCS, the NIF component SHALL process that SIP BYE message as described in Section 6.1.2.2. If, at any time, the NIF component receives a SIP BYE message from the PIF component, the NIF component SHALL process that SIP BYE message as described in Section 6.1.2.2.

C.3.2 Procedures at the ESRP

If the ESRP is stateful (i.e., has been identified in record routing), and is therefore in the path of the re-INVITE messages, the ESRP SHALL follow normal procedures, as described in RFC 3261 [10], for passing SIP re-INVITE messages and related responses (200 OK and

© Copyright 2011-2022 National Emergency Number Association, Inc.

ACK) associated with requests for Called Party Hold when the originating network and the PSAP support feature-specific signaling.

The ESRP SHALL also follow normal procedures, as described in RFC 3261 [10], for passing SIP BYE messages and Contact header fields.

C.3.3 Procedures at the i3 PSAP

If an i3 PSAP is operating in a jurisdiction in which PSAP Call Control features are supported/required, it SHALL be capable of interpreting the presence of a media feature tag[92] of "urn:emergency:media-feature.psap-call-control"[93] in a Contact header field of the original INVITE (and any subsequent requests in-dialog) as an indication from the originating network that it supports PSAP Call Control features. An i3 PSAP operating in a jurisdiction in which PSAP Call Control features are supported/required SHALL include a media feature tag of "urn:emergency:media-feature.psap-call-control" in a Contact header field of all responses (provisional or final) to that original INVITE and any subsequent requests in-dialog. If the i3 PSAP receives a media feature tag of "urn:emergency:media-feature.psap-call-control" to original INVITE messages and it is operating in a jurisdiction in which PSAP Call Control features are supported/required, the i3 PSAP MUST assume that PSAP Call Control features are in effect end-to-end. Additionally, it SHALL be capable of receiving and processing re-INVITE messages that contain new SDP offers with attribute "a= suspended" or "a=sendrecv", indicating that the re-INVITE is associated with PSAP Call Control Features. The i3 PSAP SHALL also associate re-INVITE messages that contain both a Priority header field of "emergency" and an SDP with attribute "a= inactive" or "a=sendrecv" as being associated with PSAP Call Control Features[94]. The i3 PSAP SHALL use an appropriate mechanism for notifying the PSAP attendant of the change in status.[95] (As noted above, today, this notification takes the form of a switch-hook status audible tone). In response to the change in switch-hook status, the PSAP attendant may initiate a Ringback request, using the procedures described in Section C.4.1.

---

[92] The Media feature tag SIP framework is defined in RFC 3840 [23].

[93] See Section 10.16 for registration in the NENA Registry System.

[94] The combination of Priority = "emergency" and SDP with "a=inactive" will be sent by originating networks that follow the procedures defined in PKT-SP-RSTF-C01-140314 [137] and PKT-SP-CMSS1.5-I07-120412 [138] when a caller goes on-hook and PSAP Call Control Features are in effect. (See Section C.1.2) Note that the value of the "a=" attribute within the SDP associated with these re-INVITE messages could be changed from "inactive" to "suspended" or vice-versa by SBC functionality within the ingress BCF.

[95] Details related to the mechanism used by the PSAP to notify the attendant of a change in caller status are outside the scope of this document.

© Copyright 2011-2022 National Emergency Number Association, Inc.

If an i3 PSAP is operating in a jurisdiction in which PSAP Call Control features are supported/required, and it receives a SIP BYE message from an ESRP associated with a premature disconnect, the i3 PSAP SHALL follow the procedures in RFC 3261 [10] for processing the BYE message, and MUST immediately notify the PSAP attendant of the change in status. In some circumstances, the i3 PSAP or call taker may initiate an immediate callback to the emergency caller. The callback initiated by the i3 PSAP SHALL follow the procedures specified in RFC 7090 [141] for marking the callback call by including a SIP Priority header field value of "psap-callback" in the INVITE message associated with the callback call.

C.3.4 Procedures at the Legacy PSAP Gateway

If the LPG is operating in an environment in which PSAP Call Control Features are supported, it MUST support the additional protocol and procedures described below.

C.3.4.1 Procedures at the LPG-NIF Component

The NIF component of the LPG SHALL be capable of interpreting the presence of a media feature tag of "urn:emergency:media-feature.psap-call-control" in a Contact header field of the original INVITE (and any subsequent requests in-dialog) as an indication from the originating network that it supports PSAP Call Control features. If, based on provisioning, the NIF component determines that the destination PSAP supports PSAP Call Control features, it SHALL include a media feature tag of "urn:emergency:media-feature.psap-call-control" in a Contact header field of all responses (provisional and final) to original INVITE messages and any subsequent requests in-dialog. From that point on, the NIF component of the LPG MUST assume that PSAP Call Control features are in effect end-to-end.

The NIF component of the LPG SHALL follow the procedures described in Section 6.2.2, with the following clarifications. If the NIF component of an LPG receives a re-INVITE message from an NGCS, it SHALL forward that re-INVITE to the PIF component, including an Element Identifier associated with the LPG in a Via header field (see Section 2.1.3).

If the NIF component subsequently receives a 200 OK message from the PIF component, it SHALL pass it to the NGCS, as described in Section C.3.1.1.2. Upon receiving an ACK from the NGCS, the NIF component SHALL forward the ACK to the PIF component.

If an NIF component receives a BYE message from an NGCS, it SHALL follow the procedures specified in RFC 3261 [10] for processing that message (i.e., it will return a 200 OK confirming receipt of the BYE message and terminating the session and the transaction,) however, before signaling the PIF component, the NIF component SHALL determine, based on provisioning, whether the PSAP supports PSAP Call Control Features. If the PSAP supports PSAP Call Control Features, the NIF component MUST generate a re-INVITE message containing an SDP with attribute "a = suspended" and send it to the PIF

© Copyright 2011-2022 National Emergency Number Association, Inc.

component, maintaining the connection to the PSAP. This will allow the legacy PSAP to be notified of the change in switch-hook status of the caller and allowing it to initiate Ringback if desired.

If the NIF component receives a BYE message from the NGCS and the PSAP does not support PSAP Call Control Features, the NIF component SHALL send a BYE message to the PIF component.

If the NIF component receives a BYE message from the PIF component, it SHALL follow standard RFC 3261 [10] procedures for processing the BYE and SHALL send a BYE to the NGCS.

C.3.4.2 Procedures at the LPG-PIF Component

In addition to the procedures specified in Section 6.2.1, the PIF component of the LPG SHALL be capable of receiving re-INVITE messages from the NIF component. Specifically, in the context of PSAP Call Control Features, the PIF component SHALL be capable of receiving and processing a re-INVITE message that is generated as a result of the procedures specified in Section C.3.4.1.

Upon receipt of a re-INVITE message containing an SDP with attribute "a= suspended" or a re-INVITE message containing both a "Priority= emergency" header field and an SDP with attribute "a= inactive", the PIF component of the LPG SHALL apply audio alerting to the PSAP so that the attendant is notified of the on-hook status of the emergency caller.

If the PIF component subsequently receives a re-INVITE message with a new SDP value (attribute "a= sendrecv" plus the "Priority: emergency" header field), it SHALL stop applying the on-hook status alerting, and re-establish the RTP to allow the conversation between the emergency caller and the attendant to resume.

If a PIF component receives a disconnect indication from a legacy PSAP, the PIF component SHALL follow the procedures specified in Section 6.2.4.2.1 to identify the on-hook condition as a true disconnect, then it SHALL send a BYE message to the NIF component. If the PIF component receives a BYE message from the NIF component, it SHALL apply standard RFC 3261 [10] procedures for processing the BYE message and send an on-hook signal to the PSAP.

C.3.5 Procedures at the Bridge

It is possible that a caller hangs-up intentionally or unintentionally while connected to a Bridge. When PSAP Call Control features are in effect, the caller's hook status changes must be communicated to the other participants on the conference.

© Copyright 2011-2022 National Emergency Number Association, Inc.

The following sub-sections describe how changes in the caller's hook state are propagated by the Bridge and assumes that, at a minimum the transfer-from PSAP and the callers are connected to the Bridge (refer to the appropriate sub-sections of Section 4.7 depending on the bridging method used).

C.3.5.1 Using the SIP Ad-Hoc Method

Upon receiving a switch-hook status change from the caller through a re-INVITE, the Bridge will send a NOTIFY message to the PSAP(s) that subscribed to the conference, indicating the change in the subscription state. The NOTIFY message will contain a conference data structure with a <media> element containing a <status> sub-element indicating the SDP status of the caller as received in the re-INVITE message's SDP offer a-line as per RFC 4575 [40].

C.3.5.2 Using the Route All Calls via a Conference-Aware UA Method

The procedures are the same as for the SIP Ad Hoc method.

C.4 Ringback

The Ringback feature enables the PSAP attendant to invite back an emergency caller, or someone in the surrounding area, into the conversation, over an established connection. This feature has different behaviors depending on the state of the device (on-hook or off-hook). If a conversation between an emergency caller and a PSAP attendant is occurring but the emergency caller stops responding, it allows the attendant to request that the receiver off-hook tone (also known as howler tone) be temporarily played at the caller's device. As a complement to the Called Party Hold feature, the Ringback feature also allows the attendant to request that the emergency caller's device rings if it has gone on-hook.

C.4.1 Procedures at the PSAP

If an emergency call has been established, Called Party Hold is active on that call, and the emergency caller disconnects prematurely from the call, the PSAP may wish to re-invite the caller to the call by initiating a Ringback toward that caller to trigger normal ringing of the caller's device. Likewise, if Called Party Hold is active on an existing emergency call but conversation with the emergency call has ceased abruptly, the PSAP may attempt to re-invite the emergency caller or someone else in the area to re-establish communication by initiating a Ringback towards that caller to trigger the application of howler tone.

In the case of a legacy PSAP, the attendant will typically trigger the Ringback by sending a switch-hook flash then dialing the Ringback access code (e.g., *99), resulting in DTMF signaling being sent to the LPG.

© Copyright 2011-2022 National Emergency Number Association, Inc.

In the case of an i3 PSAP, it is expected that, in response to an action taken by the attendant to request Ringback, the Ringback feature will be triggered by the PSAP UA issuing a re-INVITE with an Alert-Info header field[96] set to the appropriate audible ringing tone URI (typically, regular ringing, if the caller is considered on-hook, or ROH/howler tone, if the caller is considered off-hook) towards the emergency caller.

Note that if an i3 PSAP receives a BYE associated with an emergency call (i.e., Called Party Hold is not active on the call), and the i3 PSAP wishes to re-establish contact with the emergency caller, the i3 PSAP MAY initiate a callback to that emergency caller. The callback initiated by the i3 PSAP SHALL follow the procedures specified in RFC 7090 [141] for marking the callback call by including a SIP Priority header field value of "psap-callback" in the INVITE message associated with the callback call.

C.4.2 Procedures at the Legacy PSAP Gateway

C.4.2.1 Procedures at the LPG-PIF Component

Upon receiving a Ringback request from a legacy PSAP (in the form of a switch-hook flash and DTMF signaling generated by the attendant), the PIF component of the LPG SHALL follow the procedures defined in RFC 4733 [142] for passing DTMF signals to the NIF component of the LPG.

If the PIF component subsequently receives a 183 Session Progress message or 180 Ringing message from the NIF component (associated with an on-hook or off-hook Ringback request, as described in Section C.4.2.2) in response, it will apply audible ringing on the existing media path to the legacy PSAP.

C.4.2.2 Procedures at the LPG-NIF Component

Upon receiving DTMF information from the PIF component (using RFC 4733 [142] procedures), the NIF will interpret the DTMF information. If the NIF component determines that the DTMF information originated by the PSAP is a request for initiation of the Ringback feature, and Called Party Hold is active on the call, the NIF component SHALL generate a re-INVITE message toward the emergency caller. The re-INVITE message MUST contain an Alert-Info header field that indicates the type of alerting that should be provided. If the SDP currently associated with the call is "suspended" or "inactive" (i.e., the latest re-INVITE received by the NIF component contained an SDP with attribute "a=suspended" or

[96] Some deployments may use the P-DCS-OSPS header with a value of "RING" as defined in RFC 5503 [170] to signal Ringback. The specific method being used in one jurisdiction is determined through bilateral negotiations.

© Copyright 2011-2022 National Emergency Number Association, Inc.

an SDP attribute "a=inactive" with "Priority=emergency"), the ringing tone URI included in the Alert-Info header field SHALL be associated with regular ringing. If the SDP associated with the call has been updated in the most recently received re-INVITE message (i.e., SDP with attribute "a= sendrecv" with the "Priority: emergency" header field), the ringing tone URI in the Alert-Info header field will be associated with a receiver off-hook/howler tone to be played for a defined period.

If the Alert-Info header field sent by the NIF in the re-INVITE message is associated with regular ringing (i.e., because the caller has gone on-hook), the NIF component SHALL be capable of receiving and processing a 183 Session Progress message or 180 Ringing message in response, indicating that the emergency caller is being alerted. The NIF component SHALL pass the 183 Session Progress/180 Ringing message to the PIF component.

If the NIF component subsequently receives a 200 OK in response to the re-INVITE message it generated, the voice path SHALL be re-established between the emergency caller and the PSAP.

If the NIF component receives DTMF information from the PIF component indicating that the PSAP is requesting initiation of the Ringback feature and the connection between the LPG and the emergency caller no longer exists (because the NIF component previously received a BYE or CANCEL from the NGCS associated with the emergency call), the NIF component SHALL initiate a callback request to/towards that caller. The callback initiated by the NIF component of the LPG SHALL follow the procedures specified in RFC 7090 [141] for marking the callback call by including a SIP Priority header field value of "psap-callback" in the INVITE message associated with the callback call.

C.4.3 Procedures at the ESRP

If the ESRP is stateful (i.e., has been identified in record routing), and is therefore in the path of the re-INVITE messages, the ESRP SHALL follow normal procedures, as described in RFC 3261 [10], for passing SIP re-INVITE messages and associated responses (200 OK and ACK).

C.4.4 Procedures at the Legacy Network Gateway

C.4.4.1 Procedures at the LNG-NIF Component

The NIF component of the LNG SHALL be capable of receiving and processing a re-INVITE message that contains an Alert-Info header field. If the NIF component receives a re-INVITE message containing an Alert-Info header field associated with an emergency call that was delivered over an SS7 trunk group, the NIF component SHALL generate a SIP INFO message that includes an encapsulated SS7 FAC message with an SAP that contains

© Copyright 2011-2022 National Emergency Number Association, Inc.

a Feature Code Indicator set to "ringback request", and pass it to the PIF component (see Table 9B/T1.113.3 of GR-246-CORE [143] for details regarding the coding of the SS7 FAC message).

If the NIF component receives a re-INVITE message containing an Alert-Info header field associated with an emergency call that was delivered over an MF trunk group, the NIF component SHALL forward the re-INVITE message to the PIF component.

C.4.4.2 Procedures at the PIF Component

As described in Section C.3.1.1.1, the PIF component of the LNG SHALL be capable of receiving and processing a SIP INFO message from the NIF component. If the PIF component receives a SIP INFO containing an encapsulated FAC message from the NIF component, the PIF component SHALL generate an SS7 FAC message based on the encapsulated FAC message. In this scenario, a 180 Ringing Message SHOULD NOT be generated by the PIF component towards the NIF.

If the PIF component receives a re-INVITE message containing an Alert-Info header field, the PIF component SHALL apply alerting toward the caller appropriate for the audible ringing tone URI provided in the Alert-Info header field and SHALL return a SIP 180 Ringing message to the NIF component.

C.4.5 Procedures at the Bridge

It is possible that a caller hangs-up intentionally or unintentionally when connected to a bridge, or a caller may become unresponsive. In such circumstances, a PSAP supporting PSAP Call Control features may want to initiate a Ringback through the Bridge.

The following sub-sections describe how PSAP-originated Ringback requests are propagated by the Bridge.

C.4.5.1 Using the Ad Hoc Method

As defined in section C.4.1, PSAPs originate Ringback requests towards the caller using re-INVITE messages containing alerting information. However, when a Bridge is involved, the PSAP MUST use the REFER method to communicate with the caller via the Bridge. A PSAP that wishes to initiate a Ringback request through a Bridge MUST use the procedures defined in RFC 4579 [39] to propagate the Ringback request to the caller's leg. The REFER message associated with a Ringback request SHALL have the Refer-to header field value set to the caller's URI with a "method" parameter set to "INVITE" alongside the alerting information (i.e., either an Alert-Info or a P-DCS-OSPS header field passed as parameters). The Bridge uses the information in the REFER to initiate an INVITE message towards the

© Copyright 2011-2022 National Emergency Number Association, Inc.

caller with the alerting information. An example Refer-to header field construct would look like this:

```
Refer-To:<sip:guy@vsp.com;method=INVITE?Alert-
Info=http://localhost/howler.wav>
```

And the corresponding INVITE from the Bridge towards the caller, like this:

```
INVITE urn:service:sos SIP/2.0
From: <sip:bridge@ngcs.com>;tag=547429769-1531467798707-
To: sip:guy@vsp.com;tag=23859029fkwp42-g2486gf3w5
Call-ID: jgigjsdksdfaswdk-123412482tjf
CSeq: 155978842 INVITE
Contact: <sip:bridge@ngcs.com>
Alert-Info: <http://localhost/howler.wav>
Supported: 100rel
Allow: ACK,BYE,CANCEL,INFO,INVITE,OPTIONS,PRACK,REFER,NOTIFY,UPDATE
Accept: application/sdp,multipart/mixed
Max-Forwards: 67
```

Upon receiving a final response from the caller, the Bridge MUST send a NOTIFY message to the conference subscribers with a "sipfrag" bodypart as per RFC 3420 [33]. Subscribers can use this information to initiate an audible and/or visual indication to a call-taker that the Ringback request was submitted.

C.4.5.2 Using the Route All Calls via a Conference-Aware UA Method

The procedures are the same as for the SIP Ad Hoc method.

C.5 Enhanced Called Party Hold

As a complement to the Called Party Hold feature, Enhanced Called Party Hold allows the media path to be established even though the PSAP attendant hasn't yet answered when the caller hangs up. Once the attendant picks up, regular connection hold capabilities apply. Therefore, if the caller picks up again, his/her conversation with the attendant will automatically resume.

If a legacy originating network supports Enhanced Called Party Hold and the originating switch interconnects with the LNG via SS7 trunk groups, an ECPH timer MUST be supported at the LNG. The external signaling generated by the originating network SHOULD be the same as for Called Party Hold. The LNG SHALL follow the procedures described in Section C.5.1. The Called Party Hold procedures applicable to the ESRP, LPG, and i3 PSAP, as described in Section C.2 and its subsections, SHALL also apply for Enhanced Called Party Hold when the originating switch interconnects with the LNG via SS7-controlled trunks.

If the legacy originating network supports Enhanced Called Party Hold and the originating switch interconnects with the LNG via MF trunk groups, an ECPH timer MUST be supported

© Copyright 2011-2022 National Emergency Number Association, Inc.

at the LNG and the LNG SHALL follow the procedures described in Section C.5.2. The procedures at the ESRP, LPG, and i3 PSAP will be the same as for Enhanced Called Party Hold where SS7 trunks are used between the originating switch and the LNG.

Note that if a VoIP originating network does not support feature-specific signaling associated with PSAP Call Control Features and the caller disconnects before the PSAP attendant answers the call, a SIP CANCEL MAY be sent by the originating network. The CANCEL message SHALL be processed as specified in RFC 3261 [10] by all elements in the call path. As described in Section 4.2.1.9, if a call arrives at the ESRP but a CANCEL is received prior to any response message being received from an i3 PSAP (or LPG), such that the ESRP is unsure as to whether or not the INVITE message was ever received by the PSAP, the ESRP MUST notify the i3 PSAP (or LPG) using the AbandonedCall event.

C.5.1 Procedures at the LNG for Calls Received over SS7 Trunk Groups

C.5.1.1 Procedures at the LNG-PIF Component

When an originating switch supports Enhanced Called Party Hold and interconnects with the LNG using SS7-supported trunks, the PIF component of the LNG SHALL follow the procedures specified in Section C.3.1.1.1.

C.5.1.2 Procedures at the LNG-NIF Component

When an originating switch supports Enhanced Called Party Hold and interconnects with the LNG using SS7-controlled trunks, the NIF component of the LNG SHALL follow the procedures specified in Section C.3.1.1.2, with the following clarifications.

Upon receiving the original INVITE from the PIF, the NIF component SHALL determine, based on provisioning associated with the incoming trunk group from the originating switch, whether Enhanced Called Party Hold is supported. If supported, the NIF component MUST initiate an ECPH timer which indicates the maximum length of time that Enhanced Called Party Hold will be active. This timer should be provisionable. If ECPH is not supported, the ECPH timer MUST NOT be initiated for that call.

If the NIF subsequently receives an INFO message from the PIF component that contains an encapsulated FAC message with the Feature Code Indicator in the SAP set to "disconnect request" after a 1XX provisional response has been received but prior to receiving the 200 OK response to the original INVITE associated with the emergency call, and Enhanced Called Party Hold is supported, the NIF component SHALL generate an UPDATE message that contains an SDP offer with an "a=suspended" attribute. If the INFO message from the PIF component is received before receiving a response (provisional or final) from the NGCS, the NIF component SHALL send a CANCEL message to the NGCS and

© Copyright 2011-2022 National Emergency Number Association, Inc.

an INFO message containing an encapsulated FAC with a SAP FCI of "hold release request" to the PIF component.

If the NIF component receives a 200 OK message from the NGCS prior to the expiration of the ECPH timer, the NIF component SHALL cancel the timer and generate a SIP re-INVITE message containing an SDP with an "a= suspended" attribute, as specified in Section C.3.1.1.2. Regular Called Party Hold procedures SHALL apply from this point on.

If, based on provisioning associated with the incoming trunk group, the NIF determines that Enhanced Called Party Hold is supported, but the NIF component does not receive a 200 OK message from the NGCS prior to the expiration of the ECPH timer, the NIF SHALL send a CANCEL message to the NGCS and an INFO message containing an encapsulated FAC with an SAP FCI of "hold release request" to the PIF component.

Upon receiving the SIP INFO message with the SAP set to "disconnect request" from the PIF component where Enhanced Called Party Hold is not supported for the incoming trunk group, the NIF component SHALL send a CANCEL message to the NGCS and an INFO message containing an encapsulated FAC with an SAP FCI of "hold release request" to the PIF component.

C.5.2 Procedures at the LNG for Calls Received over MF Trunk Groups

C.5.2.1 Procedures at the LNG-PIF Component

When an originating switch supports Enhanced Called Party Hold and interconnects with the LNG using MF trunks, the PIF component of the LNG SHALL follow the procedures specified in Section C.3.1.2.1, with the following clarification. If the originating switch supports Enhanced Called Party Hold, and the caller disconnects before the emergency call is answered by the PSAP, the PIF component will receive an on-hook signal from the originating switch. The PIF component SHALL use trunk group provisioning to determine its subsequent behavior. If the provisioning associated with the incoming MF trunk group indicates that Enhanced Called Party Hold is supported, the PIF component SHALL pass the on-hook/unseize circuit telephony event to the NIF component using the mechanisms specified in RFC 5244 [140] (or equivalent).

If the emergency caller subsequently goes off-hook, the PIF component SHALL pass the off-hook/seizure telephony event to the NIF component using the mechanisms specified in RFC 5244 [140] (or equivalent).

If the provisioning associated with the incoming MF trunk group indicates that Enhanced Called Party Hold is not supported, upon receiving an on-hook signal from the originating switch, the PIF component SHALL send a CANCEL message to the NIF component and SHALL be capable of receiving and processing a 200 OK in response.

© Copyright 2011-2022 National Emergency Number Association, Inc.

C.5.2.2 Procedures at the LNG-NIF Component

When an originating switch supports Enhanced Called Party Hold and interconnects with the LNG using MF trunks, the NIF component of the LNG SHALL follow the procedures specified in Section C.3.1.2.2, with the following exceptions and clarifications.

Upon receiving the original INVITE from the PIF, the NIF component SHALL determine, based on provisioning associated with the incoming trunk group from the originating switch, whether Enhanced Called Party Hold is supported. If supported, the NIF component MUST initiate an ECPH timer which indicates the maximum length of time that Enhanced Called Party Hold will be active. This timer should be provisionable. If not supported on the incoming trunk group, the ECPH timer MUST NOT be initiated for that call.

If the NIF subsequently receives an on-hook/unseize circuit event indication from the PIF component (encoded using RFC 5244 [140] mechanisms or equivalent) after receiving a 1XX provisional response, but prior to receiving the 200 OK response to the original INVITE associated with the emergency call, and Enhanced Called Party Hold is supported, the NIF component SHALL generate an UPDATE message that contains an SDP offer with an "a=suspended" attribute. If the on-hook/unseize circuit event indication from the PIF component (encoded using RFC 5244 [140] mechanisms or equivalent) is received before receiving a response (provisional or final) from the NGCS, the NIF component SHALL send a 487 Request Terminated response message associated to the original INVITE to the PIF component and a CANCEL to the NGCS.

If Enhanced Called Party Hold is supported on the incoming MF trunk group and the NIF component receives a 200 OK message from the NGCS prior to the expiration of the ECPH timer, it SHALL cancel the timer and generate a SIP re-INVITE message containing an SDP with an "a= suspended" attribute, as specified in Section C.3.1.2.2. Regular Called Party Hold procedures SHALL apply from this point on.

If Enhanced Called Party Hold is supported on the incoming MF trunk group and the NIF component does not receive a 200 OK message from the NGCS prior to the expiration of the ECPH timer, the NIF SHALL send a 487 Request Terminated response message associated to the original INVITE to the PIF component, and a CANCEL to the NGCS.

If, based on provisioning associated with the incoming trunk group, the NIF determines that Enhanced Called Party Hold is supported, but the NIF component does not receive a 200 OK message from the NGCS prior to the expiration of the ECPH timer, the NIF SHALL send a CANCEL message to the NGCS and a 487 Request Terminated response message associated to the original INVITE to the PIF component.

Upon receiving the on-hook/unseize circuit indication from the PIF component, where Enhanced Called Party Hold is not supported for the incoming trunk group, the NIF

© Copyright 2011-2022 National Emergency Number Association, Inc.

component SHALL send a CANCEL message to the NGCS and a 487 Request Terminated response message associated to the original INVITE to the PIF component.

C.5.3 Procedures at the Bridge

It is possible that a caller hangs-up intentionally or unintentionally while being connected to a bridge.

The following sub-sections describe how a premature disconnect before call answer is propagated by the Bridge.

C.5.3.1 Using the SIP Ad Hoc Method

Given that ECPH is invoked prior to the establishment of an emergency call and that the SIP Ad Hoc Bridge is only invoked to establish a conference, which happens after initial call answer, it is impossible to encounter ECPH in the SIP Ad Hoc bridging scenario.

C.5.3.2 Using the Route All Calls via a Conference-Aware UA Method

Upon receiving a re-INVITE with updated switch-hook status prior to the issuance of the 200 OK message establishing the original emergency call session with the PSAP, the Bridge using the Conference-Aware UA method SHALL propagate the re-INVITE to the PSAP. Normal procedures for Called Party Hold/Switch-hook status defined in section C.3 ensue.

© Copyright 2011-2022 National Emergency Number Association, Inc.

Appendix D – Example Call Flows (informative)

This section provides example end-to-end i3 call flows. The first example, in Section D.1, describes a call flow in which all data is provided by value. The second example call flow, in which data is provided by reference, is presented in Section D.2. Other example calls flows may be added in future revisions of this document.

D.1 Data by Value SIP End-to-End Example Call Flow

The following assumptions and considerations have been taken in creating this example call flow:

- SIP end-to-end call;
- AIP and VSP are not vertically integrated;
- The Calling Device is nomadic;
- The Calling Device is identifiable and authenticable by the LIS to reside within its administrative domain;
- The location format is Civic;
- The provisioned location is LVF-valid in the LIS;
- The Calling UA is location-capable;
- The Calling UA is LoST-capable;
- The Calling UA has the VSP Call Server configured as its outbound proxy (by adding a Route header field pointing to the VSP CS in dialog-initiating requests[97]);
- The VSP CS is a proxy;
- Two ESInets scenario: the originating ESInet is a state/province ESInet, the terminating ESInet is a regional ESInet;
- All data is provided by-value;
- The LIS only supports HELD as a Location Configuration Protocol (LCP);
- The Policy Store is external to the ESRP but within its ESInet;
- At call time, ESRPs have already collected the Origination and Termination Policies for Queue Names they manage (enumeratePolicyRequest and response flows not shown);
- BCFs outside ESInets are not shown;
- All SIP Proxies are transaction stateful;
- Egress BCFs do not anchor media;

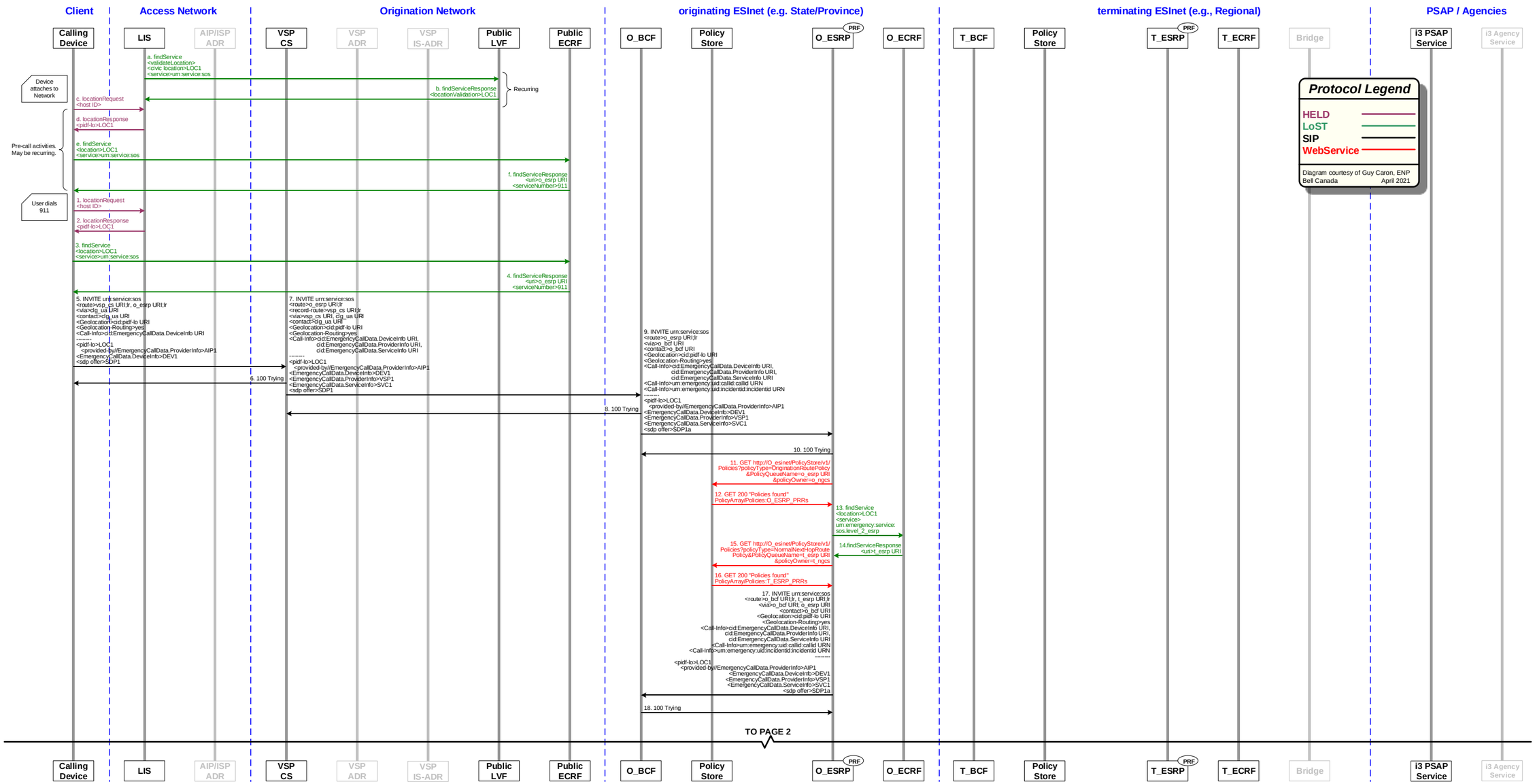
[97] Most devices don't include a Route header field with the URI of their configured outbound proxy. Rather, they just send every call to that proxy. We elected to show the header to remain strictly compliant with RFC 3261.

© Copyright 2011-2022 National Emergency Number Association, Inc.

- Ingress and egress BCFs are assumed to be the same server (shown as a single element);
- ESRPs that route calls exiting the local ESInet will send such calls to a BCF facing the desired next hop (by adding a Route header field pointing to the BCF in dialog-initiating requests);
- ECRFs return the authoritative answer, either directly or by recursion (not shown);
- All queues are in Normal State;
- PSAP and Agency are served by the same terminating (regional) ESInet;
- All elements within the ESInets have valid credentials traceable back to the PCA;
- External DNS resolution of ESRP URIs is the BCF IP address;
- Internal DNS resolution of internal ESRP URIs is the ESRP IP address;
- Provisioning, Registration, Authentication, Authorization, SIP Subscription/Notification, Logging, Recording, and Discovery flows have been omitted for simplicity;
- DNS, DHCP, and NTP flows have been omitted for simplicity;
- TCP with TLS is used for all transactions although not explicitly expressed (e.g., http vs https).

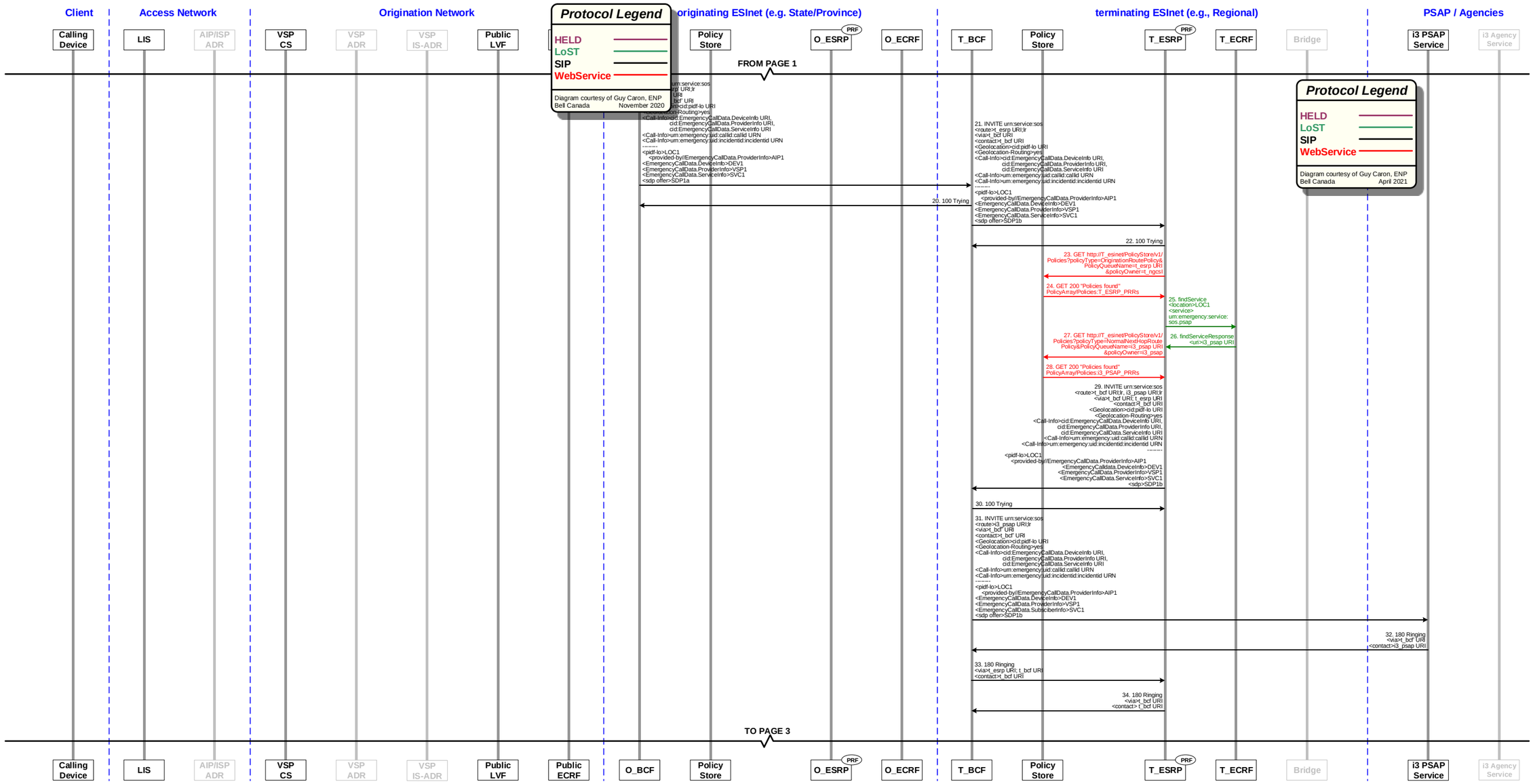
© Copyright 2011-2022 National Emergency Number Association, Inc.

Figure D1. Diagram Example i3 Call Flow – Data Provided by Value – Part 1



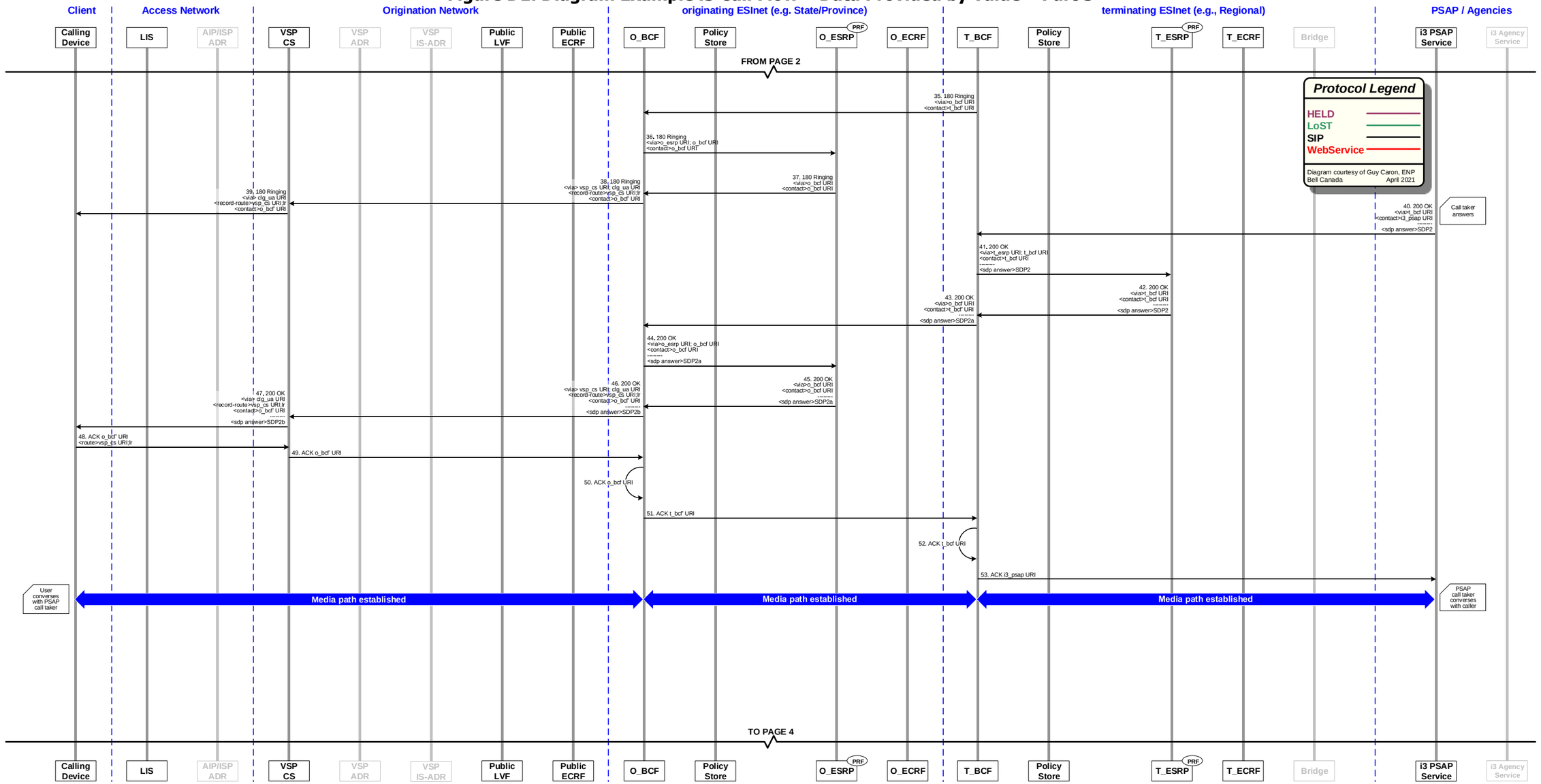
© Copyright 2011-2022 National Emergency Number Association, Inc.

Figure D1. Diagram Example i3 Call Flow – Data Provided by Value – Part 2



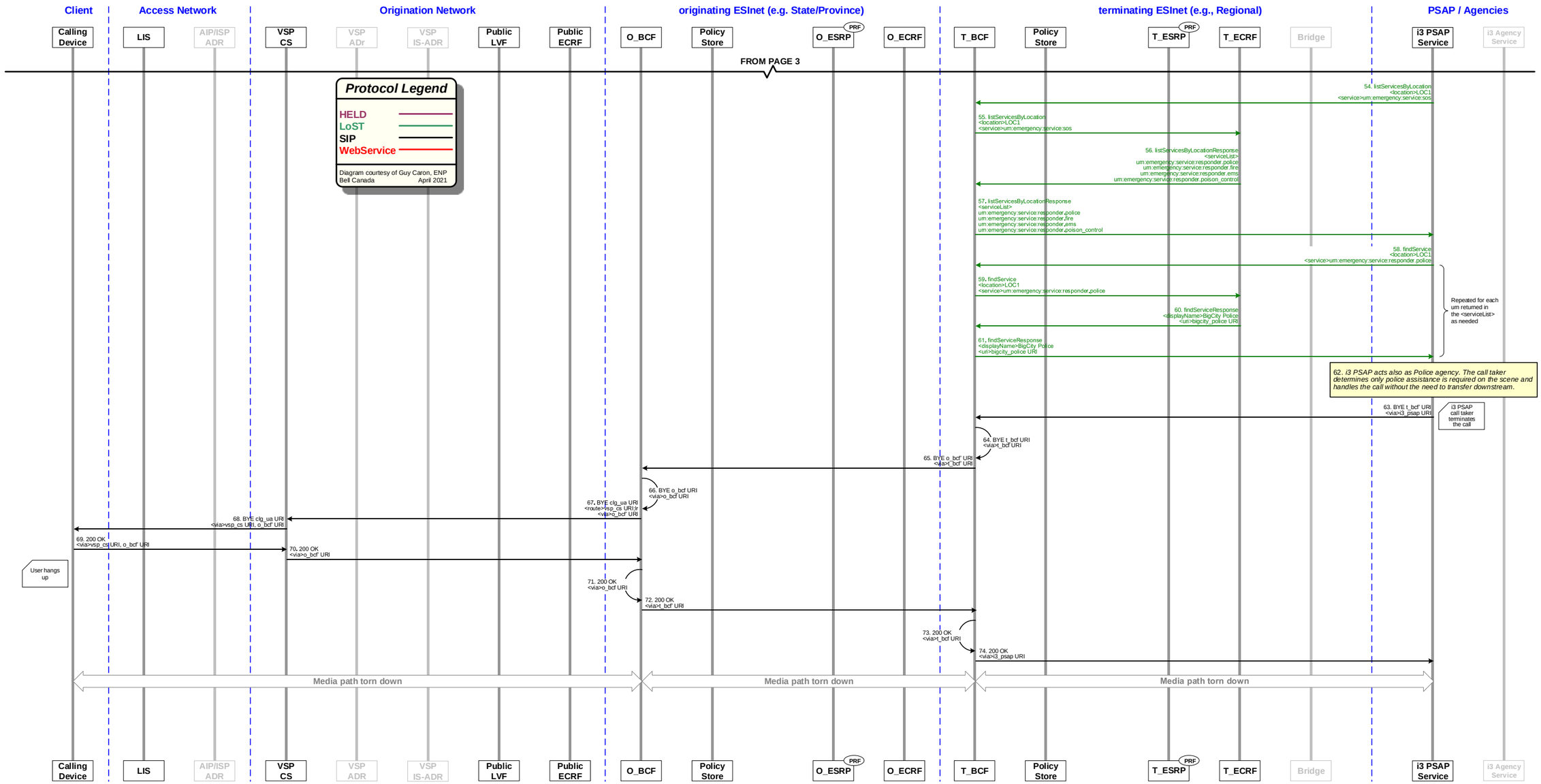
© Copyright 2011-2022 National Emergency Number Association, Inc.

Figure D1. Diagram Example i3 Call Flow – Data Provided by Value – Part 3



© Copyright 2011-2022 National Emergency Number Association, Inc.

Figure D1. Diagram Example i3 Call Flow – Data Provided by Value – Part 4



© Copyright 2011-2022 National Emergency Number Association, Inc.

D.1.1 Step-by-Step Description

D.1.1.1 Boot Up Activities (Steps Not Shown)

The LIS is statically provisioned with the URL of the Public LVF for its serving footprint. The LIS in the broadband access network has been provisioned with a record associating the location "LOC1" (which is LVF-valid) to the identifier "Host ID" of the Calling Device. The LIS exposes an external HELD interface to the network used by the Calling Device.

The nomadic Calling Device is physically connected to a broadband access network at location "LOC1".

The Calling Device boots up, attaches to the access network (i.e., it gets a service IP address and DNS server IP addresses), discovers its serving LIS and serving Public ECRF.

The SIP UA part of the Calling Device registers with its VSP (step not shown). This step may be recurring based on the settings of the UA. The VSP CS authenticates the Calling UA.

D.1.1.2 Pre-Call Activities

a. The LIS queries the public LVF with a LoST findService location validation request for the civic address "LOC1" and the service URN "urn:service:sos".
b. The Public LVF processes the validation request and returns a LoST findServiceResponse to the LIS showing "LOC1" as LVF-valid.

Steps a. and b. are recurring periodically to ensure any changes in GIS information are reflected in the LIS.

c. The Calling Device supports HELD and DHCP as Location Configuration Protocols but only the HELD request will successfully provide a location since the discovered LIS supports HELD as the LCP. The HELD locationRequest contains the Calling Device "host ID" and appropriate credentials.
d. The LIS authenticates the Calling Device (step not shown), processes the request and responds with a HELD locationResponse containing a PIDF-LO representation of civic address "LOC1", including the element <provided-by> populated with the access provider ID "AIP1".

© Copyright 2011-2022 National Emergency Number Association, Inc.

e. Using civic location "LOC1" and service URN "urn:service:sos", the Calling Device initiates a LoST findService request to the Public ECRF previously discovered. The Public ECRF does not require authentication so no credentials are provided.

f. The Public ECRF processes the request without authentication and responds with a LoST findServiceResponse containing among other things the destination URI for emergency calling <uri> "o_esrp URI" and the emergency number <serviceNumber> "911" for this area.

Steps c. to f. may recur. The rate of recurrency will be influenced by many factors associated with the device and the network to which it is attached. For example, the device may be configured to initiate a HELD locationRequest every time it is powered up and every 30 minutes thereafter. The same is true of the LoST findService request.

D.1.1.3 Call-Related Activities

1. The user is confronted with an emergency situation and uses the Calling Device to dial the emergency number he is accustomed to (in this example, 911). The Calling Device recognizes the dial string "911" as the emergency service number in the area of location "LOC1" (by comparing it to what was previously discovered in Step e), enters into "emergency calling mode", and following the advice in RFC 6881, adapts its behavior accordingly (for example, disabling certain features) and gets an updated location by querying the LIS using HELD. The HELD locationRequest contains the Calling Device "host ID" and appropriate credentials
2. The LIS authenticates the Calling Device (step not shown), processes the request, and responds with a HELD locationResponse containing a PIDF-LO representation of civic address "LOC1", including the element <provided-by> populated with the access provider ID "AIP1".
3. Using civic location "LOC1" and service URN "urn:service:sos", the Calling Device initiates a LoST findService request again to the Public ECRF previously discovered. The Public ECRF does not require authentication so no credentials are provided.
4. The Public ECRF processes the request without authentication and responds with a LoST findServiceResponse containing, among other things, the destination URI for emergency calling <uri> "o_esrp URI", and the emergency number <serviceNumber> "911" for this area.

© Copyright 2011-2022 National Emergency Number Association, Inc.

5. The Calling SIP UA sends an INVITE with the Request-URI set to "urn:service:sos", a Route header field set to the VSP CS (outbound proxy) with the "lr" parameter, another Route header field set to the value received in the LoST response of Step 2 ("o_esrp URI") augmented with the "lr" parameter, a Contact header field for itself ("clg_ua URI"), and a Geolocation header field with a cid URI pointing to the PIDF-LO document embedded in the body, along with its SDP offer "SDP1". It also includes a Call-Info header field with a purpose parameter set to "EmergencyCallData.DeviceInfo" and a cid URI pointing to Additional Data about itself in the body <EmergencyCallData.DeviceInfo> "DEV1". It also includes a Call-Info header field with a purpose parameter set to "EmergencyCallData.ProviderInfo" and a cid URI pointing to Additional Data about itself in the body <EmergencyCallData.ProviderInfo>. Both additional data body blocks contain a <DataProviderReference> element set to the same value.
6. The VSP CS receives the INVITE, authenticates the Calling UA (steps not shown), and replies with a provisional 100 Trying SIP response to the Calling UA.
7. The VSP CS recognizes the Request-URI in the INVITE set to "urn:service:sos" to be an emergency call and invokes special logic to process this message. In the forwarded INVITE, it removes the first Route header field referring to itself and adds Via and Record-Route header fields pointing to itself ("vsp_cs URI"). It also adds Call-Info header field values, each with a purpose parameter beginning with "EmergencyCallData" and cid URIs pointing to the appropriate data element in the body. It then includes the related data elements in the body, namely <EmergencyCallData.ProviderInfo> "VSP1" (additional data about the originating network or service provider), and <EmergencyCallData.SubscriberInfo> "SUB1" (additional data about the subscriber). The SDP offer "SDP1" remains since the VSP CS does not anchor media. The VSP CS performs a DNS lookup on the URI found in the Route header field ("o_esrp URI") of the incoming INVITE. The DNS resolution of this URI in the originating network returns the O_BCF IP address(es). The INVITE is forwarded there.
8. The O_BCF receives the INVITE, inspects the message for malicious content (step not shown), and replies with a provisional 100 Trying SIP response to the VSP CS. In some cases the O_BCF authenticates the VSP CS (e.g., if there is a relationship with the VSP).

© Copyright 2011-2022 National Emergency Number Association, Inc.

9. The O_BCF behaves as a full B2BUA, performs topology hiding, anchors media, and acts as the UAS for the ingress dialog. On the egress side, acting as a UAC, it creates a new transaction for the egress dialog by sending an INVITE populated with a Route header field set to "o_esrp URI;lr", Via, and Contact header fields pointing to itself ("o_bcf URI"), and an SDP offer "SDP1a". It generates Call and Incident tracking identifiers and adds them to Call-Info header fields with purpose parameters of "emergency-CallId" and "emergency-IncidentId" respectively. It also copies the Call-Info, Geolocation header field, and Geoloaction-Routing fields found in the incoming INVITE, as well as the other elements found in the body. The O_BCF then performs a DNS lookup on the URI found in the Route header field ("o_esrp URI") of the INVITE. The DNS resolution of this URI in the originating (state) ESInet returns the O_ESRP IP address(es). The INVITE is forwarded there. The O_BCF maintains independently the state of the ingress and egress dialog-initiating transactions as well as the association between them.
10. The O_ESRP receives the INVITE on the call queue associated with "o_esrp URI", authenticates the O_BCF (steps not shown), and responds with a provisional 100 Trying SIP message to the O_BCF. It deletes the top Route header field referring to it.
11. The O_ESRP is statically provisioned with the address of its Policy Store. It formulates a RetrievePolicy through an HTTP GET request to O_esinet/PolicyStore/v1/Policies (with parameters <policyType> as "OriginationRoutePolicy", "policyQueueName" as "o_esrpURI", which is the URI of the queue the call was received on and "policyOwner" as "p_ngcs", which is the Agency Identifier of the agency responsible for O_ESRP) to retrieve the originating route policies associated with it. Credentials are also provided.
12. The "O_esinet" Policy Store is provisioned with all the policies associated with its serving clients (step not shown). It receives the RetrievePolicy HTTP GET request, authenticates the O_ESRP, then dips into its database to find a record associated with the provided parameters. It returns the result in an HTTP response message with the origination route policy set for queue "o_esrp URI" in a PolicyArray object.
13. The O_ESRP invokes its internal Policy Routing Function (PRF) that processes the rules in the policy received and applies them to the incoming INVITE (step not shown). The origination policy contains the highest priority rule specifying a LoSTServiceURNCondition object which, when executed, results in a LoST query to its serving O_ECRF. The O_ESRP is provisioned with the address of the O_ECRF. It

© Copyright 2011-2022 National Emergency Number Association, Inc.

launches a LoST findService request with the following parameters: <location> "LOC1" as found in the body of the INVITE, <service> "urn:emergency:service:sos.level_2_esrp" as found in the originating policy. Credentials are also provided.

14. The O_ECRF authenticates the O_ESRP, processes the request for "LOC1" and "urn:emergency:service:sos.level_2_esrp", and returns a LoST findService Response with the URI of the next hop ("t_esrp URI") to the O_ESRP.
15. The O_ESRP receives the LoST response since the ECRF query was successful, it stores the URI received in the Normal-NextHop variable and then executes the actions associated to the rule containing the "LoSTServiceURNCondition" object. One of the actions contains an "InvokePolicyAction" actionType with "policyType" set to "NormalNexthopRoutePolicy" thus it determines it requires the route policy associated with "t_esrp URI". As such, it formulates a RetrievePolicy HTTP GET request to O_esinet/PolicyStore/v1/Policies (with parameters "policyType" as "NormalNextHopRoutePolicy" and "policyQueueName" as "t_esrp URI", which is the URI stored in the Normal-NextHop variable and "policyOwner" as "t_ngcs", which is the Agency Identifier of the agency responsible for T_ESRP) to retrieve the origination policy associated with it. Credentials are also provided.
16. The Policy Store receives the RetrievePolicy HTTP GET request, authenticates the O_ESRP, then dips into its database to find a record associated with the provided parameters. It returns the result in a response message with the route policy for queue "t_esrp URI" in a PolicyArray object.
17. The O_ESRP invokes its internal PRF that processes the rules within the policy received to determine where to send the INVITE. The route policy has a Route action that forwards the call to the normalNextHop that, in this case, is the T_ESRP. The O_ESRP adds a Route header field set to "t_esrp URI;lr" and adds a Via header field pointing to itself ("o_esrp URI"). Following its provisioned behavior for all calls exiting the local ESInet, the O_ESRP then adds a front value in the topmost Route header field pointing to its desired next hop "o_bcf URI;lr", performs a DNS lookup on it, and sends the INVITE to the O_BCF IP address.
18. The O_BCF receives the INVITE, inspects the message for malicious content, authenticates the O_ESRP (steps not shown), and replies with a provisional 100 Trying SIP response to the O_ESRP.

© Copyright 2011-2022 National Emergency Number Association, Inc.

19. The O_BCF behaves as a full B2BUA[98] and terminates the ingress dialog. On the egress side, it creates a new dialog by sending an INVITE populated with a Route header field set to "t_esrp' URI;lr", Via and Contact header fields pointing to itself ("o_bcf' URI"), and copies the Call-Info, Geolocation and Geolocation-Routing header fields, and the elements found in the body of the incoming INVITE, including the SDP offer "SDP1a". The O_BCF then performs a DNS lookup on the URI found in the Route header field ("t_esrp' URI") of the INVITE. The DNS resolution of this URI in the originating ESInet returns the T_BCF IP address(es). The INVITE is forwarded there. The O_BCF maintains independently the state of the ingress and egress dialogs as well as the association between the two dialogs.
20. The T_BCF receives the INVITE, inspects the message for malicious content, authenticates the O_BCF (steps not shown), and responds with a provisional 100 Trying SIP message to the O_BCF.
21. The T_BCF behaves as a full B2BUA[98], anchors media, and acts as the UAS for the ingress dialog. On the egress side, acting as a UAC, it creates a new transaction for the egress dialog by sending an INVITE populated with a Route header field set to "t_esrp URI;lr", Via and Contact header fields pointing to itself ("t_bcf URI"), and an SDP offer "SDP1b". It also copies the Call-Info, Geolocation and Geolocation-Routing header fields, and other elements found in the body of the incoming INVITE. The T_BCF then performs a DNS lookup on the URI found in the Route header field ("t_esrp URI") of the INVITE. The DNS resolution of this URI in the terminating (regional) ESInet returns the T_ESRP IP address(es). The INVITE is forwarded there. The T_BCF maintains independently the state of the ingress and egress dialog-initiating transactions as well as the association between them.
22. The T_ESRP receives the INVITE on the call queue associated with "t_esrp URI", authenticates the T_BCF (steps not shown), and responds with a provisional 100 Trying SIP message to the T_BCF. It deletes the top Route header field referring to it.
23. The T_ESRP is statically provisioned with the address of its Policy Store. It formulates a RetrievePolicy through an HTTP GET request to T_esinet/PolicyStore/v1/Policies (with parameters "policyType" as "OriginationRoutePolicy", "policyQueueName" as

[98] Topology hiding may occur between ESInets, but consideration should be given to not doing so in support of improved ability to diagnose problems.

© Copyright 2011-2022 National Emergency Number Association, Inc.

"t_esrp URI", which is the URI of the queue the call was received on and "policyOwner" as "t_ngcs", which is the Agency Identifier of the agency responsible for T_ESRP) to retrieve the origination route policy set associated with it. Credentials are also provided.

24. The "T_esinet" Policy Store is provisioned with all the policies associated with its serving clients (step not shown). It receives the RetrievePolicy HTTP GET request, authenticates the T_ESRP, then queries its database to find a record associated with the provided parameters. It returns the result in a response message with the origination route policy set for queue "t_esrp URI" in a PolicyArray object.
25. The T_ESRP invokes its internal Policy Routing Function (PRF) that processes the rules in the policy received and applies them to the incoming INVITE (step not shown). The origination policy contains the highest priority rule specifying a LoSTServiceURNCondition object which, when executed, results in a LoST query to its serving T_ECRF. The T_ESRP is provisioned with the address of the T_ECRF. It launches a LoST findService request with the following parameters: <location> "LOC1" as found in the body of the INVITE, <service> "urn:emergency:service:sos.psap" as found in the originating policy. Credentials are also provided.
26. The T_ECRF authenticates the T_ESRP, processes the request for "LOC1" and "urn:emergency:service:sos.psap", and returns a LoST findServiceResponse with the URI of the next hop ("i3_psap URI") to the T_ESRP.
27. The T_ESRP receives the LoST response and since the ECRF query was successful, it stores the URI received in the NormalNextHop variable and then executes the actions associated to the rule containing the "LoSTServiceURNCondition" object. One of the actions contains an "InvokePolicyAction" actionType with "policyType" set to "NormalNexthopRoutePolicy" thus it determines it requires the route policy associated with "i3_psap URI". As such, it formulates a RetrievePolicy HTTP GET request to T_esinet/PolicyStore/v1/Policies (with parameters "policyType" as "NormalNextHopRoutePolicy" and "policyQueueName" as "i3_psap URI", which is the URI stored in the NormalNextHop variable and "policyOwner" as "i3_psap", which is the Agency Identifier of the agency responsible for i3_PSAP) to retrieve the origination route policy set associated with it.. Credentials are also provided.
28. The Policy Store receives the RetrievePolicy HTTP GET request,, authenticates the T_ESRP, then queries its database to find a record associated with the provided

© Copyright 2011-2022 National Emergency Number Association, Inc.

patameters. It returns the result in a response message with the route policy for queue "i3_psap URI" in a PolicyArray object.

29. The T_ESRP invokes its internal PRF that processes the rules within the policy received to determine where to send the INVITE. The route policy has a Route action that forwards the call to the normalNextHop that, in this case, is the i3_PSAP. The T_ESRP adds a Route header field set to "i3_psap URI;lr" and adds a Via header field pointing to itself ("t_esrp URI"). Following its provisioned behavior for all calls exiting the local ESInet, the T_ESRP then adds front value in the topmost Route header field pointing to its desired next hop "t_bcf URI;lr", performs a DNS lookup on it, and sends the INVITE to the T_BCF IP address.
30. The T_BCF receives the INVITE, inspects the message for malicious content, authenticates the T_ESRP (steps not shown), and replies with a provisional 100 Trying SIP response to the T_ESRP.
31. The T_BCF behaves as a full B2BUA[98] and terminates the ingress dialog. On the egress side, it creates a new dialog by sending an INVITE populated with a Route header field set to "i3_psap URI;lr", a Via header field pointing to itself ("t_bcf' URI"), and copies the Call-Info, Geolocation and Geolocation-Routing header fields, and the elements found in the body of the incoming INVITE, including the SDP offer "SDP1b". The T_BCF then performs a DNS lookup on the URI found in the Route header field ("i3_psap URI") of the INVITE. The DNS resolution of this URI in the regional (terminating) ESInet returns the i3_PSAP IP address(es). The INVITE is forwarded there. The T_BCF maintains independently the state of the ingress and egress dialogs as well as the association between the two dialogs.
32. The i3_PSAP receives the INVITE, authenticates the T_BCF (steps not shown), presents the call on its normal call queue for the next available agent to answer, and replies with a provisional 180 Ringing[99] SIP response to the URI found in the top Via header field ("t_bcf' URI").
33. The T_BCF receives the provisional 180 Ringing message on the egress transaction and creates a reciprocal response on the ingress transaction using the Via header fields of the associated ingress INVITE pointing to the T_ESRP.

[99] The 180 Ringing message may be preceded by a 100 Trying message.

© Copyright 2011-2022 National Emergency Number Association, Inc.

34. The T_ESRP receives the provisional 180 Ringing message, removes the Via header field referring to it, and forwards the response to the URI in the next Via header field, in this case, the T_BCF.
35. The T_BCF receives the provisional 180 Ringing message on the egress dialog and creates a reciprocal response on the ingress dialog using the Via header fields of the associated ingress INVITE pointing to the O_BCF.
36. The O_BCF receives the provisional 180 Ringing message on the egress dialog and creates a reciprocal response on the ingress dialog using the Via header fields of the associated ingress INVITE pointing to the O_ESRP.
37. The O_ESRP receives the provisional 180 Ringing message, removes the Via header field referring to it, and forwards the response to the URI in the next Via header field, in this case, the O_BCF.
38. The O_BCF receives the provisional 180 Ringing message on the egress dialog and creates a reciprocal response on the ingress dialog using the Via header fields of the associated ingress INVITE pointing to the VSP CS. The O_BCF also reinstates the Record-Route header field previously received in the INVITE. It provides a different value in the Contact header field ("o_bcf' URI").
39. The VSP CS receives the provisional 180 Ringing message, removes the Via header field referring to it, and forwards the response to the URI in the next Via header field, in this case, the Calling UA.

    The Calling UA receives the provisional 180 Ringing SIP response, authenticates the VSP CS (steps not shown), processes the response, and generates a ring back tone towards the hearing medium (speaker phone, handset, headset, etc.) to alert the user that the call has reached its destination.

    Some ringing cycles later, the i3 PSAP call taker answers the call.
40. The i3 PSAP returns a final 200 OK SIP response to the URI found in the Via header field ("t_bcf' URI") with its SDP answer set to "SDP2".
41. The T_BCF receives the final 200 OK message on the egress transaction, marking the establishment of the egress dialog. It creates a reciprocal response on the ingress transaction using the Via header fields of the associated ingress INVITE pointing to the T_ESRP.

© Copyright 2011-2022 National Emergency Number Association, Inc.

42. The T_ESRP receives the final 200 OK message, removes the Via header field referring to it, and forwards the response to the URI in the next Via header field, in this case, the T_BCF.
43. The T_BCF receives the final 200 OK message on the egress transaction and creates a reciprocal response on the ingress transaction using the Via header fields of the associated ingress INVITE pointing to the O_BCF. Because it anchors media on ingress, the SDP answer is now "SDP2a". It also provides a different value in the Contact header field ("t_bcf' URI").
44. The O_BCF receives the final 200 OK message on the egress transaction and creates a reciprocal response on the ingress transaction using the Via header fields of the associated ingress INVITE pointing to the O_ESRP.
45. The O_ESRP receives the final 200 OK message, removes the Via header field referring to it, and forwards the response to the URI in the next Via header field, in this case, the O_BCF.
46. The O_BCF receives the final 200 OK message on the egress transaction and creates a reciprocal response on the ingress transaction using the Via header fields of the associated ingress INVITE pointing to the VSP CS. The O_BCF also reinstates the Record-Route header field previously received in the INVITE. Because it anchors media on ingress, the SDP answer is now "SDP2b". It also provides a different value in the Contact header field ("o_bcf' URI").
47. The VSP CS receives the final 200 OK message, removes the Via header field referring to it, and forwards the response to the URI in the next Via header field, in this case, the Calling UA.
48. The Calling UA receives the final 200 OK response, builds its route-set with the information received in the Record-Route ("vsp_cs URI"). After accepting the session media offer, it then creates an ACK request with Route header fields set to the values of its route-set. It sets the Request-URI to the value of the Contact header field ("o_bcf' URI") and sends the ACK to the top Route header field, in this case, the VSP CS.
49. The VSP CS removes the Route header field referring to it and forwards the ACK using the Request-URI ("o_bcf' URI").

© Copyright 2011-2022 National Emergency Number Association, Inc.

50. The O_BCF behaves as a full B2BUA[98]. On the egress side, it sends an ACK populated with a Request-URI set to "o_bcf URI" found in the Contact header field of the associated 200 OK response (step 44).
51. The O_BCF behaves as a full B2BUA[98] and terminates the ingress dialog. On the egress side, it uses the previously opened egress dialog and sends an ACK populated with a Request-URI set to "t_bcf' URI" found in the Contact header field of the associated 200 OK response (Step 43).
52. The T_BCF behaves as a full B2BUA[98] and terminates the ingress dialog. On the egress side, it uses the previously opened egress dialog and sends an ACK populated with a Request-URI set to "t_bcf URI" found in the Contact header field of the associated 200 OK response (Step 41).
53. The T_BCF behaves as a full B2BUA[98], performs topology hiding, and terminates the ingress dialog. On the egress side, it uses the previously opened egress dialog and sends an ACK populated with a Request-URI set to "i3_psap URI" found in the Contact header field of the associated 200 OK response (Step 40).

    Media path is established between the Calling UA and the i3 PSAP with anchoring points at the BCFs (SBC part). Conversation between the call taker and the caller commences.

54. The i3 PSAP has built-in logic to gather agency information in preparation of a potential transfer to downstream agencies. The i3 PSAP is provisioned with its serving ECRF (T_ECRF), however the T_ECRF is only reachable by a static route through the T_BCF (firewall part). The i3 PSAP sends a LoST listServicesByLocation request using "LOC1" received in the INVITE against the top-level service URN "urn:emergency:service:sos". Credentials are also provided.
55. The T_BCF (firewall part) receives the LoST request from the i3 PSAP, examines the source and destination IP addresses, inspects the message for malicious content, and lets the message go through to the T_ECRF.
56. The T_ECRF authenticates the i3 PSAP (steps not shown), processes the LoST request, dips in its database for "LOC1", and formulates a LoST listServicesByLocationResponse populated with the services available for "LOC1" ("urn:emergency:service:responder.police", "urn:emergency:service:responder.fire", "urn:emergency:service:responder.ems", and

© Copyright 2011-2022 National Emergency Number Association, Inc.

"urn:emergency:service:responder.poison_control") back to the i3 PSAP through the T_BCF.

57. The T_BCF (firewall part) receives the LoST response from the T_ECRF, examines the source and destination IP addresses, inspects the message for malicious content, and lets the message go through to the i3 PSAP.
58. With the list of available services in hand, the i3 PSAP proactively launches a LoST findServiceRequest to the T_ECRF for each of the services available. As above, the requests are sent to the T_BCF (firewall part). In this example, only the "urn:emergency:service:responder.police" service URN is shown.
59. The T_BCF (firewall part) receives the LoST request from the i3 PSAP, examines the source and destination IP addresses, inspects the message for malicious content, and lets the message go through to the T_ECRF.
60. The T_ECRF authenticates the i3 PSAP (steps not shown), processes the LoST requests, dips in its database for "LOC1" and the service URN provided in the requests (in this example, "urn:emergency:service:responder.police"), and formulates LoST findServiceResponse messages populated with the URI of the requested service along with the display name of the agency (a.k.a., English Language Translation) back to the i3 PSAP through the T_BCF.
61. The T_BCF (firewall part) receives the LoST response from the T_ECRF, examines the source and destination IP addresses, inspects the message for malicious content, and lets the message go through to the i3 PSAP.
62. The i3 PSAP acts also as the police agency. The call taker determines only police assistance is required on the scene and handles the call without the need to transfer downstream.

    Once all the information has been gathered and the caller is comforted that first responders are on their way, the call taker terminates the call (hangs up).

63.-68. Upon detecting the hang-up signal, the i3 PSAP sends a SIP BYE request towards the Calling UA. Each UAS and B2BUA uses its route-set and Contact header fields previously populated for its dialog(s) to populate the Route header fields and Request-URIs. The BYE request is propagated on the path, each element applying the routing logic gathered from the associated dialog until it reaches the Calling UA.

© Copyright 2011-2022 National Emergency Number Association, Inc.

69.-74. The Calling UA receives the BYE request and starts the tear down procedures. It then sends a final 200 OK response that gets propagated on the reverse path towards the i3 PSAP terminating the dialog and the session.

The media is torn down end-to-end. This emergency call is over.

D.2 Location by Reference / Cellular / HELD Example Call Flow

The following assumptions and considerations apply to this example call flow:

- SIP end-to-end call (e.g., on a 4G VoLTE IMS-based network);
- AIP, and VSP are the same entity (an IMS cellular provider);
- The Calling Device is mobile (an IMS cellular device);
- The cellular provider does not offer a public LIS;
- i3-required LIS functionality is provided by a Location Retrieval Function (LRF);
- The LRF (as the LIS) supports location references using HELD deref (the "pull" model);
- The location for dispatch format is geospatial;
- The Calling UA uses the P-CSCF as its outbound proxy by sending all requests to it;
- The Calling Device and originating network provide Additional Data by value[100];
- The Policy Store is external to the ESRP but within its ESInet;
- At call time, ESRPs have already collected the Origination and Termination Policies for Queue Names they manage (enumeratePolicy request and response flows not shown);
- The originating network's BCF (the IMS cellular provider, an IBCF) is not shown;
- All SIP Proxies are transaction stateful;
- Egress BCFs do not anchor media;
- ESRPs that route calls exiting the local ESInet will send such calls to a BCF facing the desired next hop (by adding a Route header field pointing to the BCF in dialog-initiating requests) (not shown);
- ECRFs return the authoritative answer, either directly or by recursion (not shown);
- All queues are in Normal State;
- PSAP and Agency are served by the same terminating (regional) ESInet;

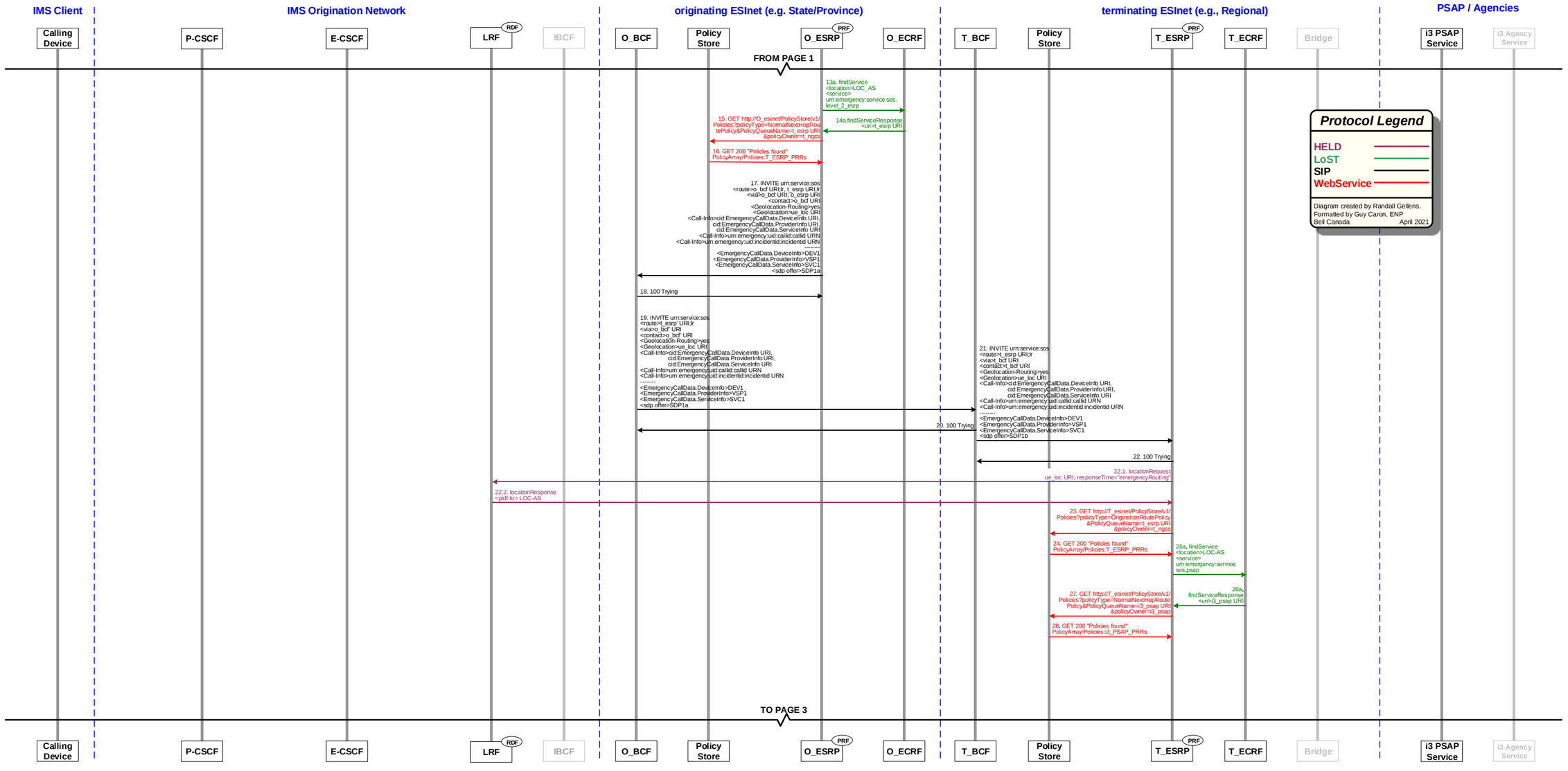
[100] It is recommended to provide Additional Data by-reference to avoid overloading the SIP INVITE. The by-value method is used here to simplify the data flow.

© Copyright 2011-2022 National Emergency Number Association, Inc.

- All elements within the ESInets have valid credentials traceable to the PCA;
- External DNS resolution of ESRP URIs returns one or more IP addresses for a BCF;
- Internal DNS resolution of internal ESRP URIs returns one or more IP addresses for an ESRP;
- DNS, DHCP, and NTP flows have been omitted for simplicity;
- TCP with TLS is used for all transactions, although not explicitly expressed (e.g., http vs https).
- The cell site to which the Calling Device is connected has an associated location (for routing), in this call flow termed "LOC-AS"; dereference of the location reference for routing returns this location.
- Prior to availability of position determination results, dereference of the location reference returns the location of the cell site to which the Calling Device is connected (in cellular terminology, a Phase I location); in this call flow termed "LOC-P1".
- An updated location estimate for the Calling Device is available after position determination (e.g., control plane or SUPL) procedures (in cellular terminology, a Phase II location); in this call flow termed "LOC-P2".
- The call-related steps in D.1 are shown; unchanged steps retain their number and additionally have "(changed)" prepended; steps that differ have a letter appended (e.g., a modified Step 1 is denoted as "1a"); additional steps have a sub-number appended (e.g., "1.1" and "1.2" denote two steps inserted after Step 1).
- The bootup and pre-call steps are entirely different since the cellular network in the example does not provide a public LIS nor use a public ECRF nor an LVF (because dispatch locations are geospatial rather than civic), and the Calling Device does not obtain its own location, nor a location reference, nor does it query a LIS or ECRF.

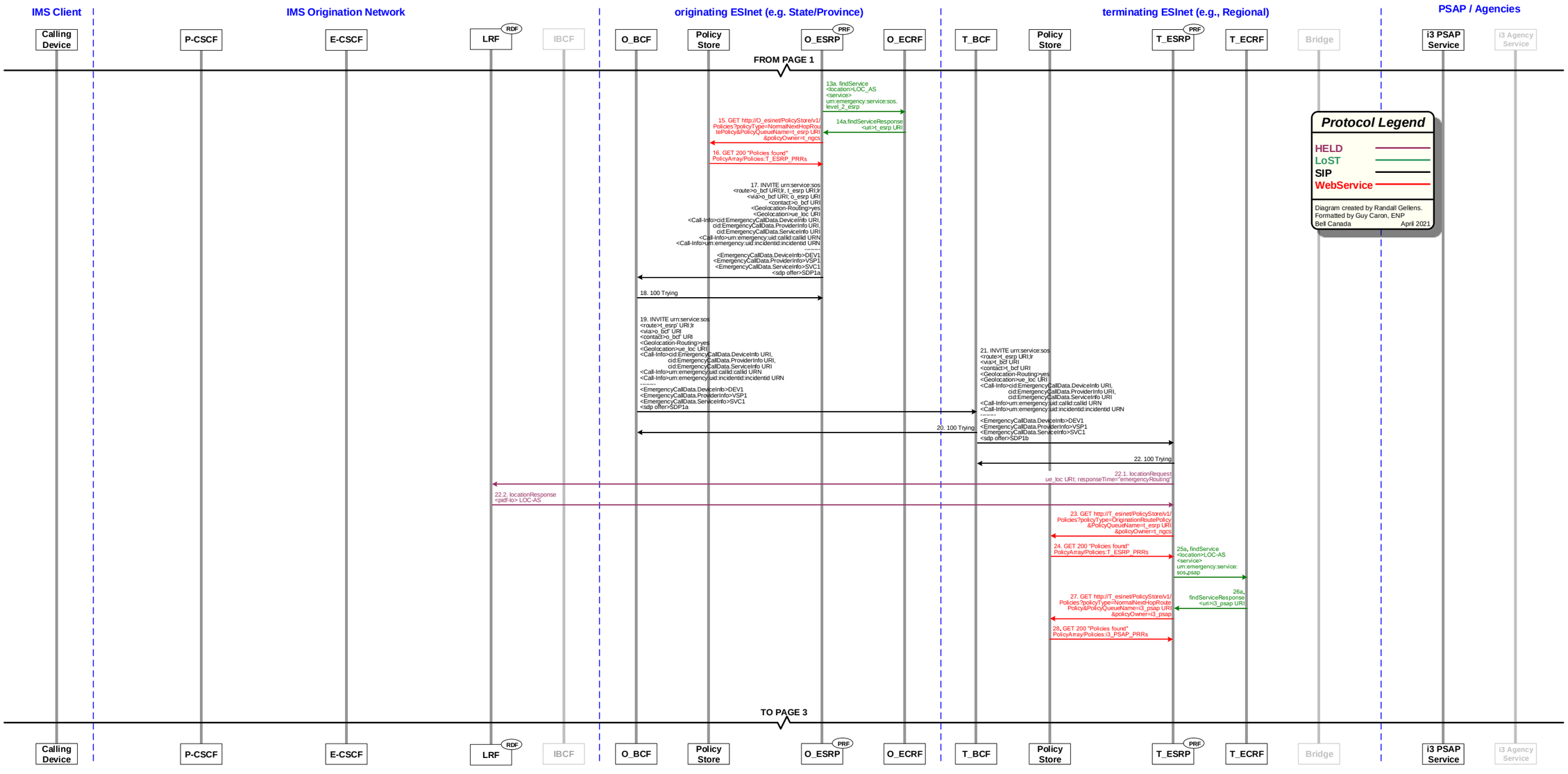
© Copyright 2011-2022 National Emergency Number Association, Inc.

Figure D2. Diagram Example i3 Call Flow – Cellular / HELD Location-by Reference – Part 1



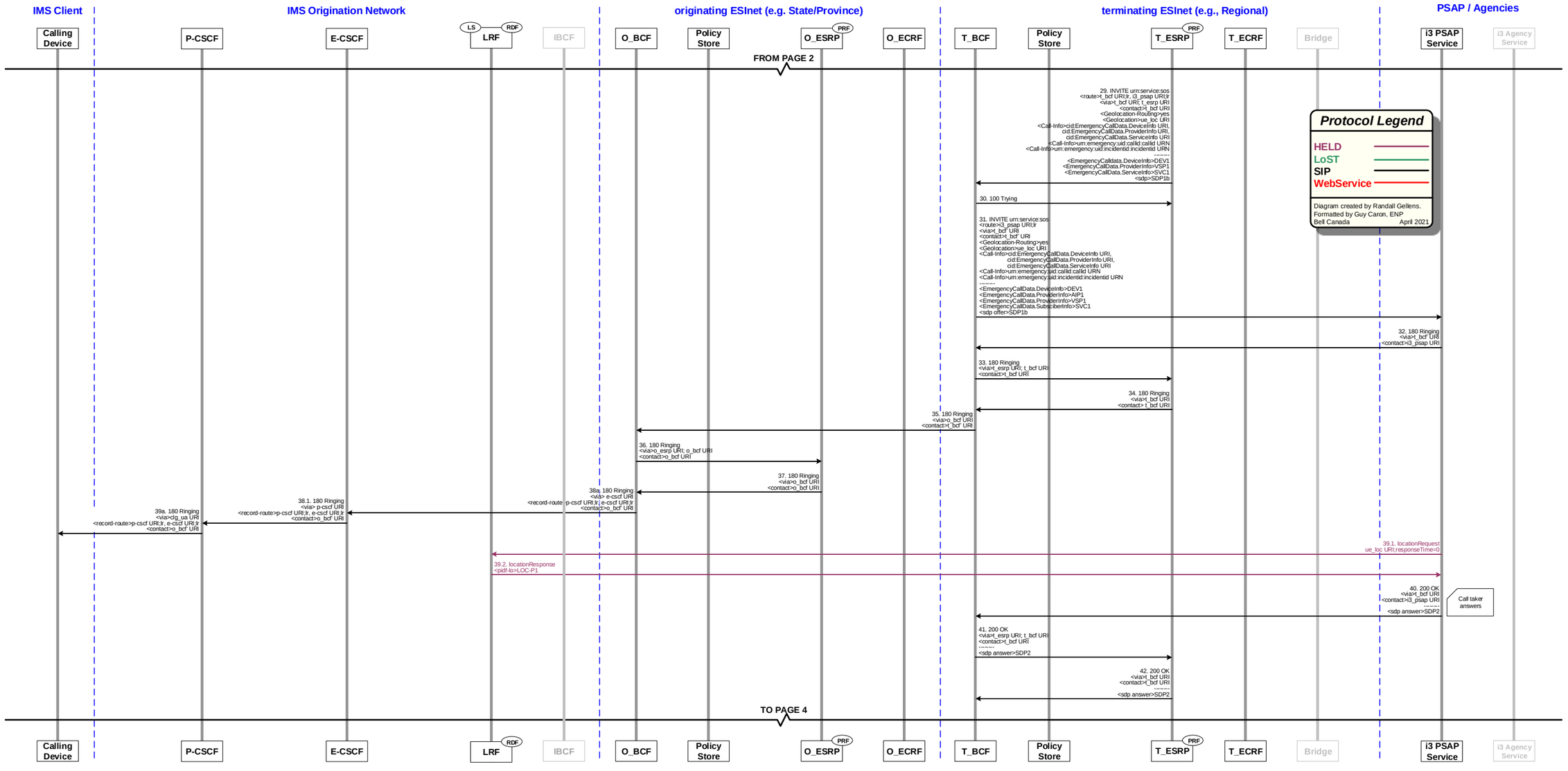
© Copyright 2011-2022 National Emergency Number Association, Inc.

Figure D2. Diagram Example i3 Call Flow – Cellular / HELD Location-by Reference – Part 2



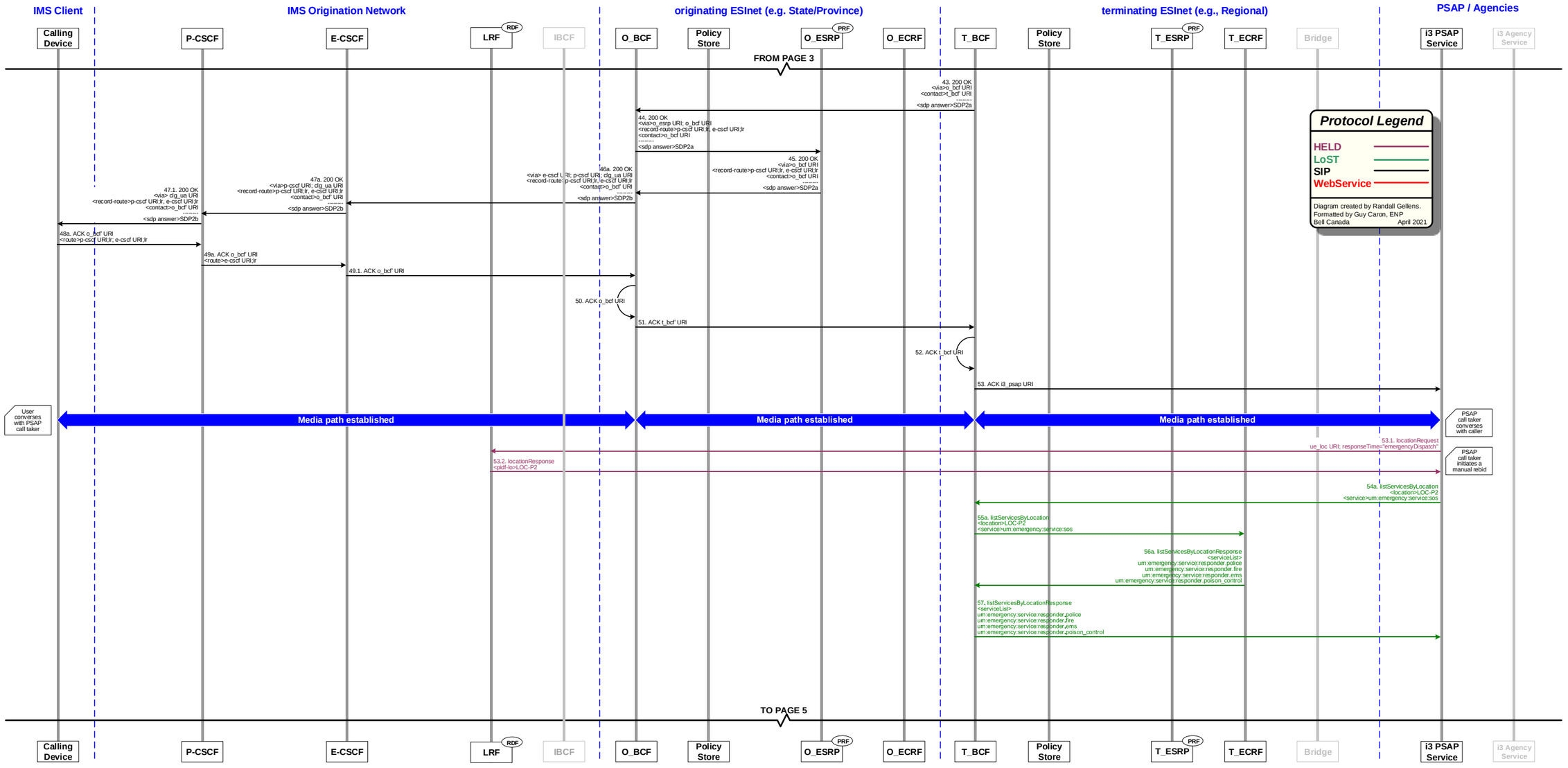
© Copyright 2011-2022 National Emergency Number Association, Inc.

Figure D2. Diagram Example i3 Call Flow – Cellular / HELD Location-by Reference – Part 3



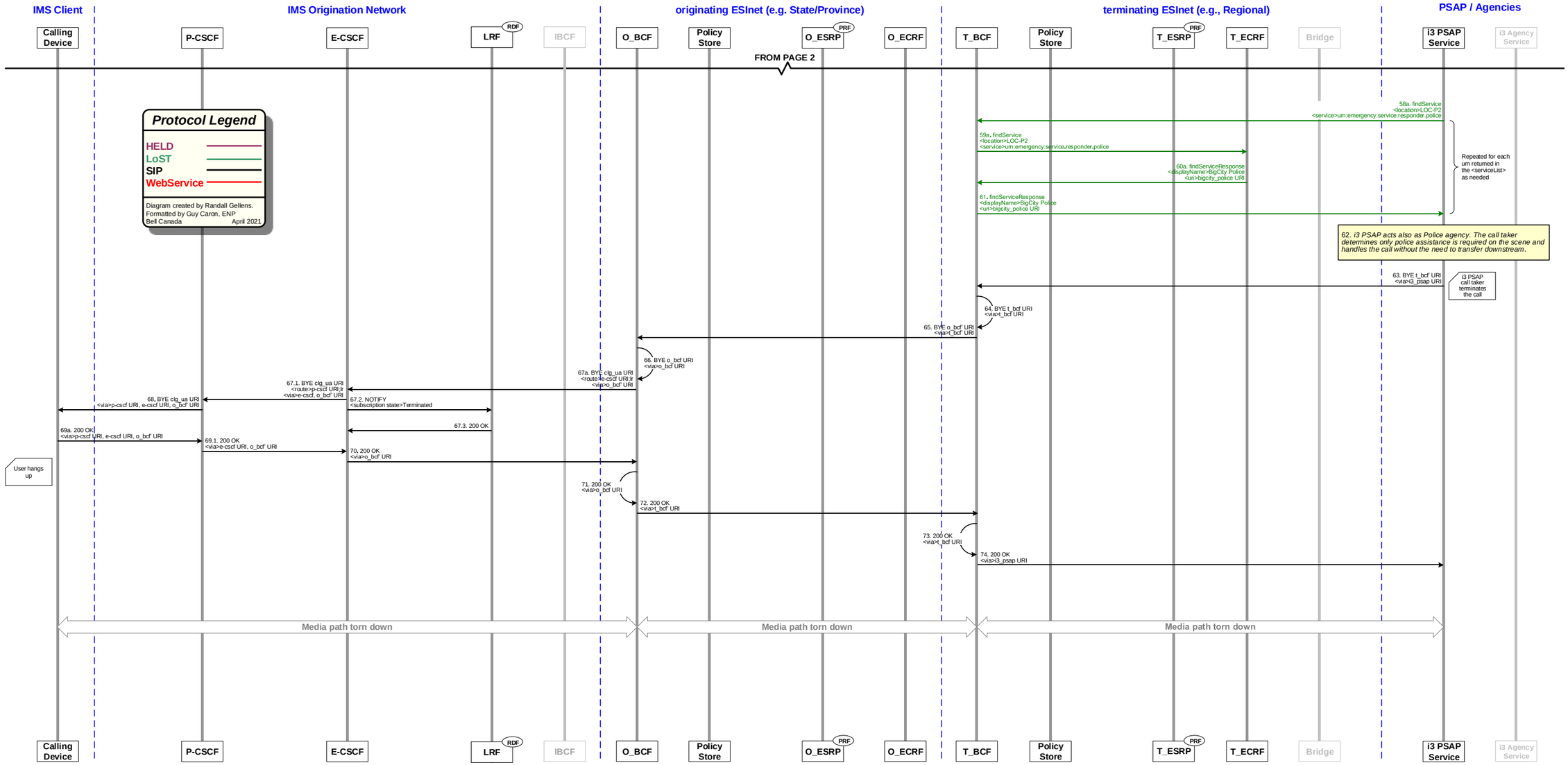
© Copyright 2011-2022 National Emergency Number Association, Inc.

Figure D2. Diagram Example i3 Call Flow – Cellular / HELD Location-by Reference – Part 4



© Copyright 2011-2022 National Emergency Number Association, Inc.

Figure D2. Diagram Example i3 Call Flow – Cellular / HELD Location-by Reference – Part 5



© Copyright 2011-2022 National Emergency Number Association, Inc.

D.2.1 Step-by-Step Description

D.2.1.1 Provisioning Activities (Steps Not Shown)

The Location Retrieval Function (LRF) in the IMS-based originating network may be provisioned with routing and Phase I static locations for the cell sectors of its serving footprint.

The Routing Determination Function (RDF) in the IMS-based originating network may be provisioned with data to assist in determining the URI based on the Associated Location [49] for routing purposes.

D.2.1.2 Pre-call Activities

a1 The Calling Device boots up, attaches to the access network (i.e., it gets a service IP address and DNS server IP addresses), and discovers its P-CSCF (and possibly also local emergency numbers). Steps not shown.

b1 If the Calling Device has credentials with the serving network, it may perform a normal (non-emergency) registration, in which case the P-CSCF communicates with the S-CSCF to authenticate the UE. Steps not shown.

D.2.1.3 Call-Related Activities

1a. The user is confronted with an emergency situation and uses the Calling Device to dial an emergency number (either a number the user is accustomed to, or a number known by the user as valid locally); in this example, 9-1-1. The Calling Device recognizes the dialstring "911" as an emergency service number (either by configuration in USIM, ISIM, etc., or by configuration information from the serving cellular network, or by static configuration), enters in "emergency calling mode" (typically, disabling certain features and enabling support for position determination mechanisms such as Control Plane or SUPL);

1.1a The Calling Device may perform an emergency registration with the P-CSCF (to obtain emergency bearer media and other emergency treatment); the P-CSCF communicates with an S-CSCF to perform this. Steps not shown;

2-4. (omitted)

5a. The Calling SIP UA sends an INVITE with the Request-URI set to "urn:service:sos", a Route header field containing the "p-cscf URI;lr", a Contact header field for itself

© Copyright 2011-2022 National Emergency Number Association, Inc.

("clg_ua URI"), a P-Access-Network-Info header field containing information about the cell it is connected via, no Geolocation header field, along with its SDP offer "SDP1". It may also include a Call-Info header field with a purpose parameter set to "EmergencyCallData.DeviceInfo" and a cid: URI pointing to Additional Data about itself in the body <EmergencyCallData.DeviceInfo> "DEV1". It may also include a Call-Info header field with a purpose parameter set to "EmergencyCallData.ProviderInfo" and a cid: URI pointing to Additional Data about itself in the body <EmergencyCallData.ProviderInfo>. If provided, these additional data body blocks contain a <DataProviderReference> element set to the same value.

6a. The P-CSCF receives the INVITE and replies with a provisional 100 Trying SIP response to the Calling UA.

6.1. The P-CSCF recognizes the Request-URI in the INVITE matching "urn:service:sos" to be an emergency call and forwards the INVITE to the E-CSCF by:

- removing the Route header field containing its own URI;
- adding a Route header field at the top of the INVITE containing a SIP URI for the E-CSCF;
- adding a Record-Route header field containing its own SIP URI;
- sending the INVITE to an IP address for the E-CSCF.

6.2. The E-CSCF:

- forwards the INVITE to the Location Retrieval Function (LRF) to obtain a route towards the PSAP, and also for the LRF to add a location reference, and also for the LRF to initiate position determination processing with the Calling Device (e.g., via control plane signaling or SUPL).

6.3. The LRF:

- creates a HELD location reference URI (ue_loc URI) for the Calling Device (e.g., an HTTPS URL with a reference created for the Calling Device for this call);
- determines a location associated with the cell currently used by the Calling Device (e.g., using a cell identified in a P-Access-Network-Info header field inserted by the UE or the P-CSCF or other network element) and sets this ("LOC-AS") as the location for routing for the Calling Device;

© Copyright 2011-2022 National Emergency Number Association, Inc.

- determines the location of the cell currently used by the Calling Device and sets this ("LOC-P1") as the initial location for the Calling Device (pending results from the positioning determination procedures);
- initiates position determination procedures with the Calling Device (e.g., using control plane or SUPL);
- obtains the route towards the PSAP based on the associated location ("LOC-AS"); the LRF consults an RDF to obtain the route (the RDF is a LoST server). Interaction with an RDF not shown.

6.4. The LRF returns a SIP 300 Multiple Choices response to the E-CSCF:

- the 300 Multiple Choices response includes a Contact header field containing a URI for the ESInet ESRP ("o_esrp URI");
- the LRF also inserts an encoded Route URI containing the o_esrp URI as a parameter of the URI in the Contact header field;
- adds a Geolocation header field containing the created location reference (ue_loc URI) as a parameter (suitably encoded) of the URI in the Contact header field;
- adds a Geolocation-Routing header field with value "yes" as a parameter (suitably encoded) of the URI in the Contact header field;
- may encode other header fields in the URI in the Contact header field.

6.5. Because the LRF needs to maintain the validity of the location reference for the Calling Device (the "ue_loc URI") for the duration of the dialog plus additional time, the LRF needs to subscribe to either the specific dialog or to all dialogs. The LRF sends a SUBSCRIBE request to the E-CSCF to receive state notifications, and the E-CSCF sends a 200 OK response to the SUBSCRIBE request, followed by an initial NOTIFY, to which the LRF responds with 200 OK. These steps not shown.

6.6. The E-CSCF receives the 300 Multiple Choices response from the LRF and updates the SIP INVITE accordingly:

- the E-CSCF decodes the header field parameters of the Contact header field and adds them to the INVITE; if the original INVITE contained Geolocation or Geolocation-Routing header fields, they are removed (replaced by the encoded header fields);
- the E-CSCF places the URI from the Contact header field URI (minus the header field parameters) of the 300 response in the topmost entry Route header field;
- the E-CSCF preserves the original Contact header field as received in the SIP INVITE from the P-CSCF.

© Copyright 2011-2022 National Emergency Number Association, Inc.

7a. The E-CSCF then:

- removes the first Route header field referring to itself;
- adds Via and Record-Route header fields pointing to itself ("e-cscf URI");
- adds a Call-Info header field and body part for <EmergencyCallData.ProviderInfo> "VSP1" (additional data about the originating network);
- optionally, adds a Call-Info header field and body part for <EmergencyCallData.ServiceInfo> "SUB1" (additional data about the service);
- (the SDP offer "SDP1" remains since neither the P-CSCF nor the E-CSCF anchors media);
- performs a DNS lookup on the o_esrp URI in the Contact header field URI set by the LRF; the DNS resolution of this URI in the originating network returns one or more O_BCF IP.

8a. The O_BCF receives the INVITE, inspects the message for malicious content (steps not shown), and replies with a provisional 100 Trying SIP response to the E-CSCF (e.g., if there is a relationship with the VSP).

9. (unchanged) The O_BCF behaves as a full B2BUA, performs topology hiding, anchors media, and acts as the UAS for the ingress dialog. On the egress side, acting as a UAC, it creates a new transaction for the egress dialog by sending an INVITE populated with a Route header field set to "o_esrp URI;lr", Via and Contact header fields pointing to itself ("o_bcf URI"), and an SDP offer "SDP1a". It generates Call and Incident tracking identifiers and adds them to Call-Info header fields with purpose parameters of "emergency-CallId" and "emergency-IncidentId", respectively. It also copies the Call-Info, Geolocation header field, and Geolocation-Routing fields found in the incoming INVITE, as well as the other elements found in the body. The O_BCF then performs a DNS lookup on the URI found in the Route header field ("o_esrp URI") of the INVITE. The DNS resolution of this URI in the originating (state) ESInet returns the O_ESRP IP address(es). The INVITE is forwarded there. The O_BCF maintains independently the state of the ingress and egress dialog-initiating transactions as well as the association between them.

10. (unchanged) The O_ESRP receives the INVITE on the call queue associated with "o_esrp URI", authenticates the O_BCF (steps not shown) and responds with a provisional 100 Trying SIP message to the O_BCF. It deletes the top Route header field referring to it.

© Copyright 2011-2022 National Emergency Number Association, Inc.

10.1. The O_ESRP resolves the ue_loc URI in the Geolocation header field to obtain a location to be used for routing: the O_ESRP sends a HELD location dereferencing request to the LRF as indicated in the ue_loc URI; the locationRequest contains a responseTime parameter set to emergencyRouting to indicate a request for location for routing.

10.2. The LRF receives the HELD location dereferencing request; because the request is for a location for routing, the LRF returns the location associated for routing with the cell ("LOC-AS") in Step 6.3; the LRF sends a HELD locationResponse containing the location "LOC-AS" to the O_ESRP.

11. (unchanged) The O_ESRP is statically provisioned with the address of its Policy Store. It formulates a RetrievePolicy through an HTTP GET request to O_esinet/PolicyStore/v1/Policies (with parameters "policyType" as "OriginationRoutePolicy", "policyQueueName" as "o_esrp URI", which is the URI of the queue the call was received on and "policyOwner" as "o_ngcs", which is the Agency Identifier of the agency responsible for O_ESRP) to retrieve the origination route policy set associated with it. Credentials are also provided.

12. (unchanged) The "O_esinet" Policy Store is provisioned with all the policies associated with its serving clients (step not shown). It receives the RetrievePolicy HTTP GET request, authenticates the O_ESRP, then dips into its database to find a record associated with the provided parameters. It returns the result in an HTTP response message with the origination route policy set for queue "o_esrp URI" in a PolicyArray object.

13a. The O_ESRP invokes its internal Policy Routing Function (PRF) that processes the rules in the policy received and applies them to the incoming INVITE (step not shown). The originating policy contains the highest priority rule specifying a LoSTServiceURNCondition object which, when executed, results in a LoST query to its serving O_ECRF. The O_ESRP is provisioned with the address of the O_ECRF. It launches a LoST findService request with the following parameters: <location> "LOC-AS" as returned in the HELD dereference, <service> "urn:emergency:service:sos.level_2_esrp" as found in the origination policy. Credentials are also provided.

14a. The O_ECRF authenticates the O_ESRP, processes the request for "LOC-AS" and "urn:emergency:service:sos.level_2_esrp", and returns a LoST findServiceResponse with the URI of the next hop ("t_esrp URI") to the O_ESRP.

© Copyright 2011-2022 National Emergency Number Association, Inc.

15. (unchanged) The O_ESRP receives the LoST response and since the ECRF query was successful, it stores the URI received in the Normal-NextHop variable and then executes the actions associated to the rule containing the "LoSTServiceURNCondition" object. One of the actions contains an "InvokePolicyAction" with "policyType" set to "NormalNexthopRoutePolicy" thus it determines it requires the route policy associated with "t_esrp URI". As such, It formulates a RetrievePolicy HTTP GET request to O_esinet/PolicyStore/v1/Policies (with parameters "policyType" as "NormalNextHopRoutePolicy" and "policyQueueName" as "t_esrp URI", which is the URI stored in the Normal-NextHop variable and "policyOwner" as "o_ngcs", which is the Agency Identifier of the agency responsible for T_ESRP) to retrieve the origination policy associated with it. Credentials are also provided.
16. (unchanged) The Policy Store receives the RetrievePolicy HTTP GET request, authenticates the O_ESRP, then dips into its database to find a record associated with the provided parameters. It returns the result in a response message with the route policy for queue "t_esrp URI" in a PolicyArray object.
17. (unchanged) The O_ESRP invokes its internal PRF that processes the rules within the policy received to determine where to send the INVITE. The route policy has a Route action that forwards the call to the normalNextHop that, in this case, is the T_ESRP. The O_ESRP adds a Route header field set to "t_esrp URI;lr" and adds a Via header field pointing to itself ("o_esrp URI"). Following its provisioned behavior for all calls exiting the local ESInet, the O_ESRP then adds a front value in the topmost Route header field pointing to its desired next hop "o_bcf URI;lr", performs a DNS lookup on it and sends the INVITE to the O_BCF IP address.
18. (unchanged) The O_BCF receives the INVITE, inspects the message for malicious content, authenticates the O_ESRP (steps not shown), and replies with a provisional 100 Trying SIP response to the O_ESRP.
19. (unchanged) The O_BCF behaves as a full B2BUA[101] and terminates the ingress dialog. On the egress side, it creates a new dialog by sending an INVITE populated with a Route header field set to "t_esrp' URI;lr", Via and Contact header fields

[101] Topology hiding may occur between ESInets, but consideration should be given to not doing so in support of improved ability to diagnose problems.

© Copyright 2011-2022 National Emergency Number Association, Inc.

pointing to itself ("o_bcf' URI"), and copies the Call-Info, Geolocation and Geolocation-Routing header fields, and the elements found in the body of the incoming INVITE, including the SDP offer "SDP1a". The O_BCF then performs a DNS lookup on the URI found in the Route header field ("t_esrp' URI") of the INVITE. The DNS resolution of this URI in the originating ESInet returns the T_BCF' IP address(es). The INVITE is forwarded there. The O_BCF maintains independently the state of the ingress and egress dialogs as well as the association between the two dialogs.

20. (unchanged) The T_BCF receives the INVITE, inspects the message for malicious content, authenticates the O_BCF (steps not shown), and responds with a provisional 100 Trying SIP message to the O_BCF.

21. (unchanged) The T_BCF behaves as a full B2BUA[101], anchors media, and acts as the UAS for the ingress dialog. On the egress side, acting as a UAC, it creates a new transaction for the egress dialog by sending an INVITE populated with a Route header field set to "t_esrp URI;lr", Via and Contact header fields pointing to itself ("t_bcf URI") and an SDP offer "SDP1b". It also copies the Call-Info, Geolocation and Geolocation-Routing header fields, and other elements found in the body of the incoming INVITE. The T_BCF then performs a DNS lookup on the URI found in the Route header field ("t_esrp URI") of the INVITE. The DNS resolution of this URI in the terminating (regional) ESInet returns the T_ESRP IP address(es). The INVITE is forwarded there. The T_BCF maintains independently the state of the ingress and egress dialog-initiating transactions as well as the association between them.

22. (unchanged) The T_ESRP receives the INVITE on the call queue associated with "t_esrp URI", authenticates the T_BCF (steps not shown), and responds with a provisional 100 Trying SIP message to the T_BCF. It deletes the top Route header field referring to it.

22.1. The T_ESRP resolves the ue_loc URI in the Geolocation header field to obtain a location to be used for routing; the T_ESRP sends a HELD location dereferencing request to the LRF as indicated in the ue_loc URI; the locationRequest contains a responseTime parameter set to emergencyRouting to indicate a request for a routing location.

22.2. The LRF receives the HELD location dereferencing request; because the request is for a routing location, the LRF returns the location associated for routing with the

© Copyright 2011-2022 National Emergency Number Association, Inc.

cell ("LOC-AS") in Step 6.3; the LRF sends a HELD locationResponse containing the location "LOC-AS" to the T_ESRP.

23. (unchanged) The T_ESRP is statically provisioned with the address of its Policy Store. It formulates a RetrievePolicy through an HTTP GET request to T_esinet/PolicyStore/v1/Policies (with parameters "policyType" as "OriginationRoutePolicy", "policyQueueName" as "t_esrp URI", which is the URI of the queue the call was received on and "policyOwner" as "t_ngcs", which is the Agency Identifier of the agency responsible for T_ESRP) to retrieve the origination route policy set associated with it. Credentials are also provided.

24. (unchanged) The "T_esinet" Policy Store is provisioned with all the policies associated with its serving clients (step not shown). It receives the RetrievePolicy HTTP GET request, authenticates the T_ESRP, then queries its database to find a record associated with the provided parameters. It returns the result in a response message with the origination route policy set for queue "t_esrp URI" in a PolicyArray object.

25a. The T_ESRP invokes its internal Policy Routing Function (PRF) that processes the rules in the policy received and applies them to the incoming INVITE (step not shown). The originating policy contains the highest priority rule specifying a LoSTServiceURNCondition object which, when executed, results in a LoST query to its serving T_ECRF. The T_ESRP is provisioned with the address of the T_ECRF. It launches a LoST findService request with the following parameters: <location> "LOC-AS" as returned in the HELD dereference, <service> "urn:emergency:service:sos.psap" as found in the originating policy. Credentials are also provided.

26a. The T_ECRF authenticates the T_ESRP, processes the request for "LOC-AS" and "urn:emergency:service:sos.psap", and returns a LoST findService Response with the URI of the next hop ("i3_psap URI") to the T_ESRP.

27. (unchanged) The T_ESRP receives the LoST response and since the ECRF query was successful, it stores the URI received in the Normal-NextHop variable and then executes the actions associated to the rule containing "LoSTServiceURNCondition" object. One of the actions contains an "InvokePolicyAction" actionType with "policyType" set to "NormalNexthopRoutePolicy" thus it determines it requires the route policy associated with "i3_psap URI". As such, it formulates a RetrievePolicy HTTP GET request to T_esinet/PolicyStore/v1/Policies (with parameters "policyType"

© Copyright 2011-2022 National Emergency Number Association, Inc.

as "NormalNextHopRoutePolicy" and "policyQueueName" as "i3_psap URI", which is the URI stored in the Normal-NextHop variable and "policyOwner" as "i3_psap", which is the Agency Identifier of the agency responsible for i3_PSAP) to retrieve the origination route policy set associated with it. Credentials are also provided.

28. (unchanged) The Policy Store receives the RetrievePolicy HTTP GET request, authenticates the T_ESRP, then queries its database to find a record associated with the provided parameters. It returns the result in a response message with the route policy for queue "i3_psap URI" in a PolicyArray object.
29. (unchanged) The T_ESRP invokes its internal PRF that processes the rules within the policy received to determine where to send the INVITE. The terminating policy has a Route action that forwards the call to the normalNextHop that, in this case, is the i3_PSAP. The T_ESRP adds a Route header field set to "i3_psap URI;lr" and adds a Via header field pointing to itself ("t_esrp URI"). Following its provisioned behavior for all calls exiting the local ESInet, the T_ESRP then adds a front value in the topmost Route header field pointing to its desired next hop "t_bcf URI;lr", performs a DNS lookup on it, and sends the INVITE to the T_BCF IP address.
30. (unchanged) The T_BCF receives the INVITE, inspects the message for malicious content, authenticates the T_ESRP (steps not shown), and replies with a provisional 100 Trying SIP response to the T_ESRP.
31. (unchanged) The T_BCF behaves as a full B2BUA[101] and terminates the ingress dialog. On the egress side, it creates a new dialog by sending an INVITE populated with a Route header field set to "i3_psap URI;lr", Via and Contact header fields pointing to itself ("t_bcf' URI"), and copies the Call-Info, Geolocation and Geolocation-Routing header fields, and the elements found in the body of the incoming INVITE, including the SDP offer "SDP1b". The T_BCF then performs a DNS lookup on the URI found in the Route header field ("i3_psap URI") of the INVITE. The DNS resolution of this URI in the regional (terminating) ESInet returns the i3_PSAP IP address(es). The INVITE is forwarded there. The T_BCF maintains independently the state of the ingress and egress dialogs as well as the association between the two dialogs.
32. (unchanged) The i3_PSAP receives the INVITE, authenticates the T_BCF (steps not shown), presents the call on its normal call queue for the next available agent to

© Copyright 2011-2022 National Emergency Number Association, Inc.

answer, and replies with a provisional 180 Ringing[102] SIP response to the URI found in the top Via header field ("t_bcf' URI").

33. (unchanged) The T_BCF receives the provisional 180 Ringing message on the egress transaction and creates a reciprocal response on the ingress transaction using the Via header fields of the associated ingress INVITE pointing to the T_ESRP.

34. (unchanged) The T_ESRP receives the provisional 180 Ringing message, removes the Via header field referring to it, and forwards the response to the URI in the next Via header field, in this case, the T_BCF.

35. (unchanged) The T_BCF receives the provisional 180 Ringing message on the egress dialog and creates a reciprocal response on the ingress dialog using the Via header fields of the associated ingress INVITE pointing to the O_BCF.

36. (unchanged) The O_BCF receives the provisional 180 Ringing message on the egress dialog and creates a reciprocal response on the ingress dialog using the Via header fields of the associated ingress INVITE pointing to the O_ESRP.

37. (unchanged) The O_ESRP receives the provisional 180 Ringing message, removes the Via header field referring to it, and forwards the response to the URI in the next Via header field, in this case, the O_BCF.

38a. The O_BCF receives the provisional 180 Ringing message on the egress dialog and creates a reciprocal response on the ingress dialog using the Via header fields of the associated ingress INVITE pointing to the E-CSCF. The O_BCF also reinstates the Record-Route header field previously received in the INVITE. It provides a different value in the Contact header field ("o_bcf' URI").

38.1. The E-CSCF receives the provisional 180 Ringing message, removes the Via header field referring to it, and forwards the response to the URI in the next Via header field, in this case, the P-CSCF.

39a. The P-CSCF receives the provisional 180 Ringing message, removes the Via header field referring to it, and forwards the response to the URI in the next Via header field, in this case, the Calling UA.

[102] The 180 Ringing message may be preceded by a 100 Trying message.

© Copyright 2011-2022 National Emergency Number Association, Inc.

The Calling UA receives the provisional 180 Ringing SIP response, processes the response, and generates a ring back tone towards the hearing medium (speaker phone, handset, headset, etc.) to alert the user that the call has reached its destination.

(unchanged) Some ringing cycles later, the i3 PSAP call taker answers the call.

39.1. The i3 PSAP has a policy of performing an initial "bid" (also referred to as an "automatic rebid") to obtain the current location information when a call taker becomes available. To do so, the i3 PSAP resolves the ue_loc URI in the Geolocation header field to obtain the current location to be used (typically Phase I) and sends an HTTPS HELD location dereferencing request to the LRF as indicated in the ue_loc URI; the locationRequest contains a responseTime parameter with a wait timer value of "0".

39.2. The LRF receives the HTTPS HELD location dereferencing request; because the request is for the current location and the position determination procedures initiated in Step 6.3 have not yet resulted in a location estimate, the LRF returns the location of the cell used by the calling device ("LOC-P1"); the LRF sends a HELD locationResponse containing the location "LOC-P1" to the i3 PSAP.

40. (unchanged) The i3 PSAP returns a final 200 OK SIP response to the URI found in the Via header field ("t_bcf' URI") with its SDP answer set to "SDP2".

41. (unchanged) The T_BCF receives the final 200 OK message on the egress transaction, marking the establishment of the egress dialog. It creates a reciprocal response on the ingress transaction using the Via header fields of the associated ingress INVITE pointing to the T_ESRP.

42. (unchanged) The T_ESRP receives the final 200 OK message, removes the Via header field referring to it, and forwards the response to the URI in the next Via header field, in this case, the T_BCF.

43. (unchanged) The T_BCF receives the final 200 OK message on the egress transaction and creates a reciprocal response on the ingress transaction using the Via header fields of the associated ingress INVITE pointing to the O_BCF. Because it anchors media on ingress, the SDP answer is now "SDP2a". It also provides a different value in the Contact header field ("t_bcf' URI").

© Copyright 2011-2022 National Emergency Number Association, Inc.

44. (unchanged) The O_BCF receives the final 200 OK message on the egress transaction and creates a reciprocal response on the ingress transaction using the Via header fields of the associated ingress INVITE pointing to the O_ESRP.

45. (unchanged) The O_ESRP receives the final 200 OK message, removes the Via header field referring to it, and forwards the response to the URI in the next Via header field, in this case, the O_BCF.

46a. The O_BCF receives the final 200 OK message on the egress transaction and creates a reciprocal response on the ingress transaction using the Via header fields of the associated ingress INVITE pointing to the E-CSCF. The O_BCF also reinstates the Record-Route header field previously received in the INVITE. Because it anchors media on ingress, the SDP answer is now "SDP2b". It also provides a different value in the Contact header field ("o_bcf' URI").

47a. The E-CSCF receives the final 200 OK message, removes the Via header field referring to itself and forwards the response to the URI in the next Via header field, in this case, the P-CSCF.

47.1. The P-CSCF receives the final 200 OK message, removes the Via header field referring to itself, and forwards the response to the URI in the next Via header field, in this case, the Calling UA.

48a. The Calling UA receives the final 200 OK response and builds its route-set with the information contained in the Record-Route header fields ("p-cscf URI;lr, e-cscf URI;lr"). After accepting the session media offer, it then creates an ACK request with Route header fields set to the values of its route-set. It sets the Request-URI to the value of the Contact header field ("o_bcf' URI") and sends the ACK to the first URI in the topmost Route header field, in this case, the P-CSCF.

49a. The P-CSCF removes the Route header field referring to itself and forwards the ACK using the Request-URI ("e-cscf URI").

49.1. The E-CSCF removes the Route header field referring to itself and forwards the ACK using the Request-URI ("o_bcf' URI").

50. (unchanged) The O_BCF behaves as a full B2BUA[101]. On the egress side, it sends an ACK populated with a Request-URI set to "o_bcf URI" found in the Contact header of the associated 200 OK response (Step 44).

51. (unchanged) The O_BCF behaves as a full B2BUA[101] and terminates the ingress dialog. On the egress side, it uses the previously opened egress dialog and sends an

© Copyright 2011-2022 National Emergency Number Association, Inc.

ACK populated with a Request-URI set to "t_bcf' URI" found in the Contact header field of the associated 200 OK response (Step 43).

52. (unchanged) The T_BCF behaves as a full B2BUA[101] and terminates the ingress dialog. On the egress side, it uses the previously opened egress dialog and sends an ACK populated with a Request-URI set to "t_bcf URI" found in the Contact header field of the associated 200 OK response (Step 41).

53. (unchanged) The T_BCF behaves as a full B2BUA, performs topology hiding, and terminates the ingress dialog. On the egress side, it uses the previously opened egress dialog and sends an ACK populated with a Request-URI set to "i3_psap URI" found in the Contact header field of the associated 200 OK response (Step 40).

(unchanged) *Media path is established between the Calling UA and the i3 PSAP with anchoring points at the BCFs (SBC part). Conversation between the call taker and the caller commences.*

53.1. The call taker initiates a manual rebid to obtain updated location information for the caller; the i3 PSAP resolves the ue_loc URI in the Geolocation header field to obtain an updated location; the i3 PSAP sends an HTTPS HELD location dereferencing request to the LRF as indicated in the ue_loc URI; the locationRequest contains a responseTime parameter set to emergencyDispatch to indicate a request for location for dispatch.

53.2. The LRF receives the HTTPS HELD location dereferencing request; the request is for a location for dispatch, and the position determination procedures initiated in Step 6.3 have resulted in at least an initial location estimate ("LOC-P2"); the LRF sends a HELD locationResponse containing the location "LOC-P2" to the i3 PSAP; position determination procedures may continue and may provide a better location estimate on a subsequent rebid.

54a. The i3 PSAP has built-in logic to gather agency information in preparation of a potential transfer to downstream agencies. The i3 PSAP is provisioned with its serving ECRF (T_ECRF), however, the T_ECRF is only reachable by a static route through the T_BCF (firewall part). The i3 PSAP sends a LoST listServicesByLocation request using the most recently received location "LOC-P2" against the top-level service URN "urn:emergency:service:sos". Credentials are also provided.

55a. The T_BCF (firewall part) receives the LoST request from the i3 PSAP, examines the source and destination IP addresses, inspects the message for malicious content,

© Copyright 2011-2022 National Emergency Number Association, Inc.

and lets the message go through to the T_ECRF. The location is LOC-P2, as the most recently received location.

56a. The T_ECRF authenticates the i3 PSAP (steps not shown), processes the LoST request, dips in its database for "LOC-P2", and formulates a LoST listServicesByLocationResponse populated with the services available for "LOC-P2" ("urn:emergency:service:responder.police", "urn:emergency:service:responder.fire", "urn:emergency:service:responder.ems", and "urn:emergency:service:responder.poison_control") back to the i3 PSAP through the T_BCF.

57. (unchanged) The T_BCF (firewall part) receives the LoST response from the T_ECRF, examines the source and destination IP addresses, inspects the message for malicious content, and lets the message go through to the i3 PSAP.

58a. With the list of available services in hand, the i3 PSAP proactively launches a LoST findServiceRequest to the T_ECRF for each of the services available. As above, the requests are sent to the T_BCF (firewall part). In this example, only the "urn:emergency:service:responder.police" service URN is shown. The location is LOC--P2.

59a. The T_BCF (firewall part) receives the LoST request from the i3 PSAP, examines the source and destination IP addresses, inspects the message for malicious content, and lets the message go through to the T_ECRF. The location remains LOC-P2.

60a. The T_ECRF authenticates the i3 PSAP (steps not shown), processes the LoST requests, dips in its database for "LOC-P2" and the service URN provided in the requests (in this example, "urn:emergency:service:responder.police"), and formulates LoST findServiceResponse messages populated with the URI of the requested service along with the display name of the agency (a.k.a., English Language Translation) back to the i3 PSAP through the T_BCF.

61. (unchanged) The T_BCF (firewall part) receives the LoST response from the T_ECRF, examines the source and destination IP addresses, inspects the message for malicious content, and lets the message go through to the i3 PSAP.

62. (unchanged) The i3 PSAP acts also as the police agency. The call taker determines only police assistance is required on the scene and handles the call without the need to transfer downstream.

© Copyright 2011-2022 National Emergency Number Association, Inc.

62.1. The call taker (who might be different from the original call taker if the call was transferred) may decide to initiate a manual rebid at any point, in which case Steps 53.1 and 53.2 are repeated. Steps not shown.

Once all the information has been gathered and the caller is comforted that first responders are on their way, the call taker terminates the call (hangs up).

63.-68. Upon detecting the hang-up signal, the i3 PSAP sends a SIP BYE request towards the Calling UA. Each UAS and B2BUA uses its route-set and Contact header fields previously populated for its dialog(s) to populate the Route header fields and Request-URIs. The BYE request is propagated on the path, each element applying the routing logic gathered from the associated dialog until it reaches the Calling UA. These steps are unchanged from D.1 except that instead of transiting the VSP CS, the signaling transits the E-CSCF and P-CSCF (Steps 67a, 67.1, 68a). In addition, upon receiving the BYE, the E-CSCF sends a last NOTIFY to the LRF and terminates the subscription created in Step 6.5 (Steps 67.2 and 67.3).

69.-74. (unchanged) The Calling UA receives the BYE request and starts the tear down procedures. It then sends a final 200 OK response that gets propagated on the reverse path towards the i3 PSAP terminating the dialog and the session.

The media is torn down end-to-end. This emergency call is over.

© Copyright 2011-2022 National Emergency Number Association, Inc.

Appendix E - REST/JSON Definitions (Normative)

Web Services defined in this document are described using OpenAPI V3, with JSON-ld exchange schemas for NIEM conformance. This section contains the OpenAPI interface definition as a YAML object. Examples of each interface are provided (future).

E.1 Policy Store

E.1.1 OpenAPI Interface Description

```
openapi: 3.0.1
info:
  title: Policy Store
  version: "1.0"
servers:
  - url: http://localhost/PolicyStore/v1
paths:
  /Policies:
    get:
      tags:
        - RetrievePolicy, UpdatedPolicy
      summary: Retrieves all policies from the store. Use limit and start
parameters for pagination.
      operationId: RetrievePolicy
      parameters:
        - name: limit
          in: query
          description: Maximum number of results to return
          required: false
          schema:
            type: integer
            format: int32
        - name: start
          in: query
          description: First item in the page of results, as an ordinal 1-
based integer
          required: false
          schema:
            type: integer
            format: int32
            minimum: 1
        - name: policyOwner
          in: query
          description: ID of the Agency owning policy(ies)
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
            required: false
            schema:
              type: string
          - name: policyType
            in: query
            description: Type of the policy
            required: false
            schema:
              type: string
          - name: policyQueueName
            in: query
            description: Policy queue name
            required: false
            schema:
              type: string
              format: uri
          - name: policyId
            in: query
            description: Id of the policy
            required: false
            schema:
              type: string
        responses:
          '200':
            description: Policies found
            content:
              application/json:
                schema:
                  $ref: '#/components/schemas/PolicyArray'
          '307':
            description: Temporary Redirect
            headers:
              Location:
                description: Referral URI of another Policy Store which may
store the policy requested
                schema:
                  type: string
          '404':
            description: Not found
          '451':
            description: Unknown or bad Policy Type
          '452':
            description: Unknown or bad Agency Name
          '453':
            description: Not available here, no referral available
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
        '454':
          description: Unspecified Error
    post:
      tags:
        - CreatePolicy
      summary: Creates a new policy in the Policy Store
      operationId: CreatePolicy
      requestBody:
        description: Policy to add (JWS using flattened JSON
serialization)
        content:
          application/json:
            schema:
              $ref: 'i3-common.yaml#/components/schemas/Jws'
        required: true
      responses:
        '201':
          description: Policy successfully created
        '434':
          description: Signature Verification Failure
        '436':
          description: Duplicate or Invalid Priority
        '437':
          description: Bad Policy Structure
        '438':
          description: Unacceptable Algorithm
        '451':
          description: Unknown or bad Policy Type
        '452':
          description: Unknown or bad Agency Name
        '454':
          description: Unspecified Error
        '459':
          description: Bad policyExpirationTime
    put:
      tags:
        - UpdatePolicy
      summary: Updates an existing policy. In order to identify a policy
the following parameters must be specified - policyType, policyQueueName
OR policyId.
      operationId: UpdatePolicy
      parameters:
        - name: policyOwner
          in: query
          description: Owner of the policy
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
            required: true
            schema:
              type: string
          - name: policyType
            in: query
            description: Type of the policy
            required: true
            schema:
              type: string
          - name: policyQueueName
            in: query
            description: Policy queue name
            required: false
            schema:
              type: string
              format: uri
          - name: policyId
            in: query
            description: Id of the policy
            required: false
            schema:
              type: string
        requestBody:
          description: Policy to update (JWS using flattened JSON
serialization)
          content:
            application/json:
              schema:
                $ref: 'i3-common.yaml#/components/schemas/Jws'
          required: true
        responses:
          '200':
            description: Policy successfully updated
          '404':
            description: Not found
          '434':
            description: Signature Verification Failure
          '436':
            description: Duplicate or Invalid Priority
          '437':
            description: Bad Policy Structure
          '451':
            description: Unknown or bad Policy Type
          '452':
            description: Unknown or bad Agency Name
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
        '454':
          description: Unspecified Error
        '460':
          description: Bad PolicyExpirationTime
    delete:
      tags:
        - DeletePolicy
      summary: Deletes an existing policy. In order to identify a policy
the following parameters must be specified - policyType, policyQueueName
OR policyId.
      operationId: DeletePolicy
      parameters:
        - name: policyOwner
          in: query
          description: Owner of the policy
          required: true
          schema:
            type: string
        - name: policyType
          in: query
          description: Type of the policy
          required: true
          schema:
            type: string
        - name: policyQueueName
          in: query
          description: Policy queue name
          required: false
          schema:
            type: string
            format: uri
        - name: policyId
          in: query
          description: Id of the policy
          required: false
          schema:
            type: string
      responses:
        '200':
          description: Policy successfully deleted
        '404':
          description: Not found
        '451':
          description: Unknown or bad Policy Type
        '452':
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
          description: Unknown or bad Agency Name
        '454':
          description: Unspecified Error
  /PolicyEnums:
    get:
      tags:
        - EnumeratePolicy
      summary: Returns a list of policy types available in the store for a
specific agency/service. Use limit and start parameters for pagination.
      operationId: EnumeratePolicy
      parameters:
        - name: limit
          in: query
          description: Maximum number of results to return
          required: false
          schema:
            type: integer
            format: int32
        - name: start
          in: query
          description: First item in the page of results, as an ordinal 1-
based integer
          required: false
          schema:
            type: integer
            format: int32
            minimum: 1
        - name: policyOwner
          in: query
          description: ID of the Agency owning policy(ies)
          required: false
          schema:
            type: string
        - name: policyType
          in: query
          description: Type of the policy
          required: true
          schema:
            type: string
        - name: policyQueueName
          in: query
          description: Policy queue name
          required: false
          schema:
            type: string
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
            format: uri
          - name: policyId
            in: query
            description: Id of the policy
            required: false
            schema:
              type: string
          - name: policiesUpdatedSince
            in: query
            description: The query will return all policies having the time
of creation or last modification greater than policiesUpdatedSince
            required: false
            schema:
              type: string
              format: date-time
              example: '2020-03-10T10:00:00-05:00'
        responses:
          '200':
            description: Policies enumerations found
            content:
              application/json:
                schema:
                  $ref: '#/components/schemas/PolicyEnumArray'
          '404':
            description: Not found
          '451':
            description: Unknown or bad Policy Type
          '452':
            description: Unknown or bad Agency Name
          '454':
            description: Unspecified Error
    /Versions:
      servers:
        - url: https://api.example.com/PolicyStore
          description: Override base path for Versions query
      get:
        tags:
          - RetrieveVersions
        summary: Retrieves all supported versions, vendor parameter is
optional.
        operationId: RetrieveVersions
        responses:
          '200':
            description: Versions found
            content:
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
            application/json:
              schema:
                $ref: 'i3-common.yaml#/components/schemas/VersionsArray'
components:
  schemas:
    PolicyArray:
      type: object
      required:
        - count
        - totalCount
        - policies
      properties:
        count:
          type: integer
          format: int32
          description: Number of items in the array
        totalCount:
          type: integer
          format: int32
          description: Total number of items found
        policies:
          type: array
          items:
            $ref: 'i3-common.yaml#/components/schemas/Jws'
          description: Array of Policy objects, each in JWS format (JWS
using flattened JSON serialization)
    Policy:
      type: object
      required:
        - policyType
        - policyOwner
        - policyRules
      properties:
        policyType:
          type: string
          description: Values limited to those in the policyType registry
        policyOwner:
          type: string
        policyQueueName:
          type: string
          format: uri
        policyId:
          type: string
        policyExpirationTime:
          type: string
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
        format: date-time
        example: '2020-03-10T10:00:00-05:00'
      policyRules:
        type: array
        items:
          $ref: '#/components/schemas/Rule'
      policyLastModificationTime:
        type: string
        format: date-time
        example: '2020-03-10T10:00:00-05:00'
      description:
        type: string
PolicyEnumArray:
  type: object
  required:
    - count
    - totalCount
    - policyEnums
  properties:
    count:
      type: integer
      format: int32
      description: Number of items in the array
    totalCount:
      type: integer
      format: int32
      description: Total number of items found
    policyEnums:
      type: array
      items:
        $ref: '#/components/schemas/PolicyEnum'
      description: Array of Policy Enums objects
PolicyEnum:
  type: object
  required:
    - policyType
    - policyOwner
    - policyExpirationTime
    - policyLastModificationTime
  properties:
    policyType:
      type: string
    policyOwner:
      type: string
    policyQueueName:
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
            type: string
            format: uri
          policyId:
            type: string
          policyExpirationTime:
            type: string
            format: date-time
            example: '2020-03-10T10:00:00-05:00'
          policyLastModificationTime:
            type: string
            format: date-time
            example: '2020-03-10T10:00:00-05:00'
      Rule:
        type: object
        required:
          - id
          - priority
          - actions
        properties:
          id:
            type: string
            description: Unique ID within a Policy,
          priority:
            type: integer
            format: int32
            minimum: 0
          conditions:
            type: array
            items:
              $ref: '#/components/schemas/Condition'
          actions:
            type: array
            items:
              $ref: '#/components/schemas/Action'
          description:
            type: string
      Action:
        type: object
        required:
          - actionType
        properties:
          actionType:
            type: string
            enum: [RouteAction, NotifyAction, LogAction, BusyAction,
  InvokePolicyAction]
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
        description:
          type: string
      discriminator:
        propertyName: actionType
    RouteAction:
      allOf:
        - $ref: '#/components/schemas/Action'
        - type: object
          required:
            - recipientUri
          properties:
            recipientUri:
              type: string
              format: uri
            rnaTimer:
              type: integer
              format: int32
            cause:
              type: string
    NotifyAction:
      allOf:
        - $ref: '#/components/schemas/Action'
        - type: object
          required:
            - eventCode
            - urgency
          properties:
            recipient:
              type: string
              format: uri
            eventCode:
              type: string
              description: Values limited to those in the
EsrpNotifyEventCodes registry
            urgency:
              type: integer
              format: int32
            comment:
              type: string
    BusyAction:
      allOf:
        - $ref: '#/components/schemas/Action'
    LogAction:
      allOf:
        - $ref: '#/components/schemas/Action'
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
      - type: object
        required:
          - message
        properties:
          message:
            type: string
  InvokePolicyAction:
    allOf:
      - $ref: '#/components/schemas/Action'
      - type: object
        required:
          - policyType
        properties:
          policyType:
            type: string
          policyQueueName:
            type: string
            format: uri
          policyId:
            type: string
  Condition:
    type: object
    required:
      - conditionType
    properties:
      conditionType:
        $ref: 'i3-common.yaml#/components/schemas/ConditionType'
      negation:
        type: boolean
      description:
        type: string
    discriminator:
      propertyName: conditionType
  TimePeriodCondition:
    allOf:
      - $ref: '#/components/schemas/Condition'
      - type: object
        required:
          - dateStart
          - dateEnd
        properties:
          dateStart:
            type: string
            format: date-time
            example: '2019-11-04T02:00:00-05:00'
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
          dateEnd:
            type: string
            format: date-time
            example: '2020-03-10T01:59:59-05:00'
          timeStart:
            type: string
            example: '08:00:00'
          timeEnd:
            type: string
            example: '18:00:00'
          weekdayList:
            type: string
            example: 'MO,TU,WE,TH,FR'
    SipHeaderCondition:
      allOf:
        - $ref: '#/components/schemas/Condition'
        - type: object
          required:
            - field
            - operator
            - content
          properties:
            field:
              type: string
            operator:
              type: string
              enum: [EQ, SS, IS]
            content:
              type: string
    AdditionalDataCondition:
      allOf:
        - $ref: '#/components/schemas/Condition'
        - type: object
          required:
            - type
            - operator
          properties:
            type:
              type: string
            element:
              type: string
            operator:
              type: string
              enum: [exists, missing, EQ, SS, NE, GT, LT, GE, LE]
            content:
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
          type: string
MimeBodyCondition:
  allOf:
    - $ref: '#/components/schemas/Condition'
    - type: object
      required:
        - mimeList
      properties:
        mimeList:
          type: array
          items:
            type: string
LocationCondition:
  allOf:
    - $ref: '#/components/schemas/Condition'
    - type: object
      required:
        - location
      properties:
        location:
          type: object
          required:
            - lo
            - profile
            - label
            - lang
          properties:
            lo:
              type: string
            profile:
              type: string
              enum: [civic, geodetic]
            label:
              type: string
            lang:
              type: string
            extension:
              type: object
        extension:
          type: object
CallSuspicionCondition:
  allOf:
    - $ref: '#/components/schemas/Condition'
    - type: object
      required:
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
            - scoreFrom
            - scoreTo
          properties:
            scoreFrom:
              type: integer
              format: int32
            scoreTo:
              type: integer
              format: int32
    SecurityPostureCondition:
      allOf:
        - $ref: '#/components/schemas/Condition'
        - type: object
          required:
            - service
            - condition
            - value
          properties:
            service:
              type: string
            condition:
              type: string
              enum: [EQ, NE]
            value:
              type: string
              description: Values limited to those in the SecurityPosture
registry
    QueueStateCondition:
      allOf:
        - $ref: '#/components/schemas/Condition'
        - type: object
          required:
            - queue
            - condition
            - value
          properties:
            queue:
              type: string
              format: uri
            condition:
              type: string
              enum: [EQ, NE]
            value:
              type: string
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
              description: Values limited to those in the QueueState
registry
    LostServiceUrnCondition:
      allOf:
        - $ref: '#/components/schemas/Condition'
        - type: object
          required:
            - urn
          properties:
            urn:
              type: string
    ServiceStateCondition:
      allOf:
        - $ref: '#/components/schemas/Condition'
        - type: object
          required:
            - service
            - condition
            - value
          properties:
            service:
              type: string
            condition:
              type: string
              enum: [EQ, NE]
            value:
              type: string
              description: Values limited to those in the serviceState
registry
    CallSourceCondition:
      allOf:
        - $ref: '#/components/schemas/Condition'
        - type: object
          required:
            - operator
            - content
          properties:
            operator:
              type: string
              enum: [EQ, SS, NE]
            content:
              type: string
    BodyPartCondition:
      allOf:
        - $ref: '#/components/schemas/Condition'
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
      - type: object
        required:
          - contentType
          - element
          - operator
          - content
        properties:
          contentType:
            type: string
          element:
            type: string
          operator:
            type: string
            enum: [EQ, SS, NE, GT, LT, GE, LE, exists, missing]
          content:
            type: string
RequestUriCondition:
  allOf:
    - $ref: '#/components/schemas/Condition'
    - type: object
      required:
        - operator
        - content
      properties:
        operator:
          type: string
          enum: [EQ, SS, NE]
        content:
          type: string
NormalNextHopCondition:
  allOf:
    - $ref: '#/components/schemas/Condition'
    - type: object
      required:
        - operator
        - content
      properties:
        operator:
          type: string
          enum: [EQ, SS, NE]
        content:
          type: string
IncomingQueueCondition:
  allOf:
    - $ref: '#/components/schemas/Condition'
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
      - type: object
        required:
          - operator
          - content
        properties:
          operator:
            type: string
            enum: [EQ, SS, NE]
          content:
            type: string
            format: uri
  SdpOfferCondition:
    allOf:
      - $ref: '#/components/schemas/Condition'
      - type: object
        properties:
          video:
            type: boolean
          audio:
            type: boolean
          rtt:
            type: boolean
          im:
            type: boolean
          text:
            type: boolean
          langVideo:
            type: array
            items:
              type: string
          langAudio:
            type: array
            items:
              type: string
          langRtt:
            type: array
            items:
              type: string
          langIm:
            type: array
            items:
              type: string
          langText:
            type: array
            items:
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
                type: string
            langVideoPref:
              $ref: '#/components/schemas/Pref'
            langAudioPref:
              $ref: '#/components/schemas/Pref'
            langRttPref:
              $ref: '#/components/schemas/Pref'
            langImPref:
              $ref: '#/components/schemas/Pref'
            langTextPref:
              $ref: '#/components/schemas/Pref'
    CapCondition:
      allOf:
        - $ref: '#/components/schemas/Condition'
        - type: object
          required:
            - tag
          properties:
            tag:
              type: string
              enum: [Identifier, Sender, Address, InfoEventCode,
InfoValueName]
            operator:
              type: string
              enum: [EQ, SS, NE]
            content:
              type: string
            nonInteractive:
              type: boolean
    CallingNumberVerificationStatusCondition:
      allOf:
        - $ref: '#/components/schemas/Condition'
        - type: object
          required:
            - operator
            - content
          properties:
            operator:
              type: string
              enum: [EQ, NE]
            content:
              type: string
    Pref:
      type: object
      required:
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
        - langList
        - langTest
      properties:
        langList:
          type: string
        langTest:
          type: string
```

E.1.2 Examples

E.2 Discrepancy Report

E.2.1 OpenAPI Interface Description

```
openapi: 3.0.1
info:
  title: Discrepancy Reports Service
  version: "1.0"
servers:
  - url: http://localhost/DiscrepancyReports/v1
paths:
  /Reports:
    post:
      tags:
        - SubmitReport
      summary: Submits a new Discrepancy Report
      operationId: SubmitReport
      requestBody:
        description: Discrepancy Report data
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/DiscrepancyReport'
        required: true
      callbacks:
        submitResolution:
          '{#/components/schemas/DiscrepancyReport/resolutionUri}':
            post:
              requestBody:
                required: true
                content:
                  application/json:
                    schema:
                      $ref: '#/components/schemas/DiscrepancyResolution'
              responses:
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
                '201':
                  description: Resolution received
      responses:
        '201':
          description: Report successfully created
          content:
            application/json:
              schema:
                $ref: '#/components/schemas/DiscrepancyReportResponse'
        '454':
          description: Unspecified Error
        '470':
          description: Unknown Service/Database ("not ours")
        '471':
          description: Unauthorized Reporter
  /Resolutions:
    post:
      tags:
        - SubmitResolution
      summary: Submits a new Discrepancy Resolution
      operationId: SubmitResolutiuon
      requestBody:
        description: Discrepancy Resolution data
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/DiscrepancyResolution'
        required: true
      responses:
        '201':
          description: Discrepancy Resolution successfully created
        '454':
          description: Unspecified Error
        '472':
          description: Unauthorized Responder
        '473':
          description: Unknown ReportId
    get:
      tags:
        - GetResolution
      summary: Retrieves a Discrepancy Report Resolution based on Agency
Name and Discrepancy Report ID
      operationId: GetResolution
      parameters:
        - name: agencyName
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
            in: query
            description: Reporting Agency Name
            required: true
            schema:
              type: string
          - name: discrepancyReportId
            in: query
            description: ID of the Discrepancy Report
            required: true
            schema:
              type: string
        responses:
          '200':
            description: Resolution found
            content:
              application/json:
                schema:
                  $ref: '#/components/schemas/DiscrepancyResolution'
          '404':
            description: Not found
          '471':
            description: Unauthorized Reporter
          '473':
            description: Unknown ReportId
          '475':
            description: Response not available yet
    /StatusUpdates:
      get:
        tags:
          - StatusUpdateRequest
        summary: Request a Status Update for a previously submitted
  Discrepancy Report
        operationId: StatusUpdateRequest
        parameters:
          - name: agencyName
            in: query
            description: Reporting Agency Name
            required: true
            schema:
              type: string
          - name: discrepancyReportId
            in: query
            description: ID of the Discrepancy Report
            required: true
            schema:
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
            type: string
      responses:
        '200':
          description: Status Update found
          content:
            application/json:
              schema:
                $ref: '#/components/schemas/StatusUpdate'
        '404':
          description: Not found
        '454':
          description: Unspecified Error
        '471':
          description: Unauthorized Reporter
        '473':
          description: Unknown ReportId
        '474':
          description: Resolution already provided
  /Versions:
    servers:
      - url: https://api.example.com/DiscrepancyReports
        description: Override base path for Versions query
    get:
      tags:
        - RetrieveVersions
      summary: Retrieves all supported versions, vendor parameter is
optional.
      operationId: RetrieveVersions
      responses:
        '200':
          description: Versions found
          content:
            application/json:
              schema:
                $ref: 'i3-common.yaml#/components/schemas/VersionsArray'
components:
  schemas:
    DiscrepancyReport:
      type: object
      required:
        - resolutionUri
        - reportType
        - discrepancyReportSubmitTimeStamp
        - discrepancyReportId
        - reportingAgencyName
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
        - reportingContactJcard
        - problemSeverity
      properties:
        resolutionUri:
          type: string
          format: uri
          example: https://agencyX.com/DiscrepancyReports/resolutions
        reportType:
          type: string
          enum: [PolicyStoreDiscrepancyReport, LostDiscrepancyReport,
BcfDiscrepancyReport, LoggingDiscrepancyReport,
CallTakerDiscrepancyReport,
                SipDiscrepancyReport, PermissionsDiscrepancyReport,
GisDiscrepancyReport, LisDiscrepancyReport, PolicyDiscrepancyReport,
                OriginatingServiceDiscrepancyReport,
CallTransferDiscrepancyReport, McsDiscrepancyReport,
EsrpDiscrepancyReport, AdrDiscrepancyReport,
                NetworkDiscrepancyReport, ImrDiscrepancyReport,
TestCallDiscrepancyReport, LogSignatureCertificateDiscrepancyReport]
        discrepancyReportSubmitTimeStamp:
          type: string
          format: date-time
          example: '2020-03-10T10:00:00-05:00'
        discrepancyReportId:
          type: string
        reportingAgencyName:
          type: string
        reportingAgentId:
          type: string
        reportingContactJcard:
          type: string
        problemService:
          type: string
        problemSeverity:
          type: string
        problemComments:
          type: string
      discriminator:
        propertyName: reportType
    DiscrepancyReportResponse:
      type: object
      required:
        - respondingAgencyName
        - respondingContactJcard
      properties:
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
      respondingAgencyName:
        type: string
      respondingContactJcard:
        type: string
      respondingAgentId:
        type: string
      responseEstimatedReturnTime:
        type: string
        format: date-time
        example: '2020-03-10T10:00:00-05:00'
      responseComments:
        type: string
  DiscrepancyResolution:
    type: object
    required:
      - respondingAgencyName
      - respondingContactJcard
      - discrepancyReportId
      - reportingAgencyName
      - problemService
      - responseTime
      - resolution
    properties:
      respondingAgencyName:
        type: string
      respondingContactJcard:
        type: string
      respondingAgentId:
        type: string
      discrepancyReportId:
        type: string
      reportingAgencyName:
        type: string
      problemService:
        type: string
      responseTime:
        type: string
        format: date-time
        example: '2020-03-10T10:00:00-05:00'
      reportingAgentId:
        type: string
      responseComments:
        type: string
      resolution:
        type: string
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
          enum: [DiscrepancyCorrected, NoDiscrepancy, OtherResponse,
PolicyAdded, PolicyUpdated, NoSuchPolicy, InsufficientCredentials,
EntryAdded,
                 PerPolicy, CallTakerAdvised, TransferCorrect,
BadCertificateChain, DataCorrected, RecordsCorrected,
PermissionsCorrected,
                 DeviceConfigError, PolicyCorrected, NoError,
ProblemCorrected, InvalidRecord, Gis, Acknowledged, OtherResponse]
    StatusUpdate:
      type: object
      required:
        - respondingAgencyName
        - respondingContactJcard
        - responseEstimatedReturnTime
      properties:
        respondingAgencyName:
          type: string
        respondingContactJcard:
          type: string
        respondingAgentId:
          type: string
        responseEstimatedReturnTime:
          type: string
          format: date-time
          example: '2020-03-10T10:00:00-05:00'
        statusComments:
          type: string
    PolicyStoreDiscrepancyReport:
      allOf:
        - $ref: '#/components/schemas/DiscrepancyReport'
        - type: object
          required:
            - policyAgencyName
            - problem
            - retrievePolicyResponse
          properties:
            policyType:
              type: string
            policyQueueName:
              type: string
            policyId:
              type: string
            policyAgencyName:
              type: string
            problem:
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
              type: string
              enum: [PolicyInvalid, PolicyAltered,
SignatureVerificationFailure, PolicyMissing, OtherPolicyStore]
            retrievePolicyResponse:
              type: string
    LostDiscrepancyReport:
      allOf:
        - $ref: '#/components/schemas/DiscrepancyReport'
        - type: object
          required:
            - query
            - request
            - response
            - problem
          properties:
            query:
              type: string
              enum: [findService, getServiceBoundary, listServices,
listServicesByLocation]
            request:
              type: string
            response:
              type: string
            problem:
              type: string
              enum: [BelievedValid, BelievedInvalid, NoSuchLocation,
RouteIncorrect, MultipleMappings, ServiceBoundaryIncorrect,
ServiceNumberIncorrect, DataExpired, IncorrectUri, LocationErrorInError,
OtherLost]
            discrepancyDetail:
              type: string
    BcfDiscrepancyReport:
      allOf:
        - $ref: '#/components/schemas/DiscrepancyReport'
        - type: object
          required:
            - problem
            - sosSource
            - eventTimestamp
          properties:
            request:
              type: string
            problem:
              type: string
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
              enum: [InitialTrafficBlocked, MidTrafficBlocked, BadSdp,
BadSip, MediaLoss, TrafficNotBlockedBadActor, TrafficNotBlocked, Qos,
BadCdr, Tty, Firewall, OtherBcf]
            sosSource:
              type: string
              format: byte
            eventTimestamp:
              type: string
              format: date-time
              example: '2020-03-10T10:00:00-05:00'
            packetHeader:
              type: string
    LoggingDiscrepancyReport:
      allOf:
        - $ref: '#/components/schemas/DiscrepancyReport'
        - type: object
          required:
            - request
            - problem
            - result
          properties:
            request:
              type: string
            problem:
              type: string
              enum: [InviteSrsError, LogEventError, RetrieveLogEventError,
OtherLogging]
            result:
              type: string
            callIdUrn:
              type: string
            incidentIdUrn:
              type: string
    CallTakerDiscrepancyReport:
      allOf:
        - $ref: '#/components/schemas/DiscrepancyReport'
        - type: object
          required:
            - callIdUrn
            - incidentIdUrn
            - pidfLo
            - callHeader
          properties:
            callIdUrn:
              type: string
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
            incidentIdUrn:
              type: string
            pidfLo:
              type: string
            callHeader:
              type: string
    SipDiscrepancyReport:
      allOf:
        - $ref: '#/components/schemas/DiscrepancyReport'
        - type: object
          required:
            - problem
          properties:
            problem:
              type: string
              enum: [InitialINVITE, MESSAGE, OPTIONS, MidDialog,
RequiredMedia, MediaProblem, EngorgedQ, Signaling, OtherSip]
            callIdUrn:
              type: string
            incidentIdUrn:
              type: string
            testCallGenerator:
              type: string
            request:
              type: string
            result:
              type: string
            queueName:
              type: string
    PermissionsDiscrepancyReport:
      allOf:
        - $ref: '#/components/schemas/DiscrepancyReport'
        - type: object
          required:
            - problem
            - resource
            - identity
            - result
          properties:
            problem:
              type: string
              enum: [UnableAuthenticate, UnableSubscribe, AbleSubscribe,
UnableRead, UnableWrite, UnableDelete, AbleRead, AbleWrite, AbleDelete,
OtherPermissions]
            resource:
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
              type: string
            identity:
              type: string
            result:
              type: string
            detail:
              type: string
    GisDiscrepancyReport:
      allOf:
        - $ref: '#/components/schemas/DiscrepancyReport'
        - type: object
          required:
            - problem
          properties:
            problem:
              type: string
              enum: [Gap, Overlap, IncorrectLost, BadGeometry,
DuplicateAttribute, OmittedField, IncorrectDataType, AddressRange,
GeneralProvisioning, MalformedUri, DisplayData, OtherGis]
            layerIds:
              type: string
            location:
              type: string
            lostUri:
              type: string
              format: uri
            detail:
              type: string
    LisDiscrepancyReport:
      allOf:
        - $ref: '#/components/schemas/DiscrepancyReport'
        - type: object
          required:
            - problem
          properties:
            problem:
              type: string
              enum: [IncorrectRecords, OwnLocationUnavailable,
LocationReferenceNotResolved, BadPidfLo, IncorrectLocation, OtherLis]
            ownLocationRequest:
              type: string
            locationUrn:
              type: string
            pidfLo:
              type: string
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
    PolicyDiscrepancyReport:
      allOf:
        - $ref: '#/components/schemas/DiscrepancyReport'
        - type: object
          required:
            - policyId
          properties:
            policyId:
              type: string
            problem:
              type: string
              enum: [InvalidUrn, UnknownPSAP, ConflictingRoute,
OtherConflict, IncorrectUrn, Malformed, Loop, VerificationFailure,
OtherPolicy]
            location:
              type: string
            callId:
              type: string
            routeUrn:
              type: string
    OriginatingServiceDiscrepancyReport:
      allOf:
        - $ref: '#/components/schemas/DiscrepancyReport'
        - type: object
          required:
            - problem
          properties:
            problem:
              type: string
              enum: [LocationNotLvfValid, LocationNotUsable, NoAni,
BadPidfLo, QueryTimeOut, CallDropped, IncorrectLocation, BadSip,
CallDrought, CallFlood, InvalidAdr, BadAdditionalData, OtherOsp, StiError]
            status:
              type: string
            location:
              type: string
            locationId:
              type: string
            locationCorrect:
              type: string
            callHeader:
              type: string
            callVolume:
              type: integer
              format: int32
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
        callVolumeTimePeriod:
          type: integer
          format: int32
CallTransferDiscrepancyReport:
  allOf:
    - $ref: '#/components/schemas/DiscrepancyReport'
    - type: object
      required:
        - callId
        - incidentId
        - origin
        - status
        - destination
      properties:
        callId:
          type: string
        incidentId:
          type: string
        origin:
          type: string
        status:
          type: string
        destination:
          type: string
McsDiscrepancyReport:
  allOf:
    - $ref: '#/components/schemas/DiscrepancyReport'
    - type: object
      required:
        - serviceCall
        - pidfLo
        - msag
        - statusCode
      properties:
        serviceCall:
          type: string
        pidfLo:
          type: string
        msag:
          type: string
        statusCode:
          type: string
        referral:
          type: string
EsrpDiscrepancyReport:
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
      allOf:
        - $ref: '#/components/schemas/DiscrepancyReport'
        - type: object
          required:
            - problem
          properties:
            problem:
              type: string
              enum: [CallReceived, EngorgedQ, CallDrought]
            callId:
              type: string
            incidentId:
              type: string
            pidfLo:
              type: string
            queueName:
              type: string
    AdrDiscrepancyReport:
      allOf:
        - $ref: '#/components/schemas/DiscrepancyReport'
        - type: object
          required:
            - problem
          properties:
            problem:
              type: string
              enum: [ReferenceNotResolved, Malformed, UnknownBlock,
ReceivedIncorrectData, TooManyUris, OtherAdr]
            block:
              type: string
            location:
              type: string
            identity:
              type: string
            url:
              type: string
              format: uri
            result:
              type: string
    NetworkDiscrepancyReport:
      allOf:
        - $ref: '#/components/schemas/DiscrepancyReport'
        - type: object
          required:
            - problem
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
            - timestamp
          properties:
            problem:
              type: string
              enum: [ReferenceNotResolved, Malformed, UnknownBlock,
ReceivedIncorrectData, TooManyUris, OtherAdr]
            ipAddressLocal:
              type: string
              format: ipv4
            ipAddressRemote:
              type: string
              format: ipv4
            url:
              type: string
              format: uri
            timestamp:
              type: string
              format: date-time
              example: '2020-03-10T10:00:00-05:00'
    ImrDiscrepancyReport:
      allOf:
        - $ref: '#/components/schemas/DiscrepancyReport'
        - type: object
          required:
            - problem
            - callId
            - callHeader
          properties:
            problem:
              type: string
              enum: [EngorgedQ, ResponseIncorrect, ResponseConfusing,
CallTransferIncorrect, ExcessiveSilence, UnknownScript, InputFailed,
ScriptLogicFailure, OtherImr]
            callId:
              type: string
            incidentId:
              type: string
            callHeader:
              type: string
    TestCallDiscrepancyReport:
      allOf:
        - $ref: '#/components/schemas/DiscrepancyReport'
        - type: object
          required:
            - problem
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
            - callIdUrn
            - request
            - nbrOfCalls
            - successCount
            - failCount
            - time
            - result
            - mediaOk
          properties:
            problem:
              type: string
              enum: [TestInvite, TestMessage, TestOptions, TestMidDialog,
TestMedia, TestLoopbackMedia, TestSignaling, OtherTestCall]
            callIdUrn:
              type: string
              format: uri
            request:
              type: string
            nbrOfCalls:
              type: integer
              format: int32
            successCount:
              type: integer
              format: int32
            failCount:
              type: integer
              format: int32
            time:
              type: string
              format: date-time
              example: '2020-03-10T10:00:00-05:00'
            result:
              type: integer
              format: int32
            contact:
              type: string
            sdp:
              type: string
            mediaOk:
              type: boolean
    LogSignatureCertificateDiscrepancyReport:
      allOf:
        - $ref: '#/components/schemas/DiscrepancyReport'
        - type: object
          required:
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
            - problem
            - logIdentifier
          properties:
            problem:
              type: string
              enum: [BadAlgorithm, NoCert, BadURL, BadThumb, BadCertX5c,
BadCertX5u, BadSignature, OtherLogSignature]
            logIdentifier:
              type: string
            result:
              type: string
            thumbCalc:
              type: string
```

E.2.2 Examples

E.3 Dequeue Registration

E.3.1 OpenAPI Interface Description

```
openapi: 3.0.1
info:
  title: Dequeue Registration Service
  version: "1.0"
servers:
  - url: http://localhost/DequeueRegistration/v1
paths:
  /Registrations:
    put:
      tags:
        - DequeueRegistration
      summary: Registers or deregisters an entity as a dequeuer
      operationId: DequeueRegistration
      requestBody:
        description: Registration details
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/Registration'
        required: true
      responses:
        '200':
          description: Registration successfully updated/created
          content:
            application/json:
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
              schema:
                type: object
                properties:
                  expirationTime:
                    type: integer
                    format: int32
                    description: Time in seconds this registration will
expire.
        '400':
          description: Bad request
        '454':
          description: Unspecified Error
        '456':
          description: Bad queue
        '457':
          description: Bad dequeuePreference
        '458':
          description: Policy violation
  /Versions:
    servers:
      - url: https://api.example.com/DequeueRegistration
        description: Override base path for Versions query
    get:
      tags:
        - RetrieveVersions
      summary: Retrieves all supported versions, vendor parameter is
optional.
      operationId: RetrieveVersions
      responses:
        '200':
          description: Versions found
          content:
            application/json:
              schema:
                $ref: 'i3-common.yaml#/components/schemas/VersionsArray'
components:
  schemas:
    Registration:
      type: object
      required:
        - queueUri
        - dequeuerUri
        - expirationTime
      properties:
        queueUri:
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
            type: string
            format: uri
          dequeuerUri:
            type: string
            format: uri
          expirationTime:
            type: integer
            format: int32
            description: Time in seconds this registration will expire.
expirationTime set to zero is a request to deregister.
          dequeuePreference:
            type: integer
            format: int32
            minimum: 1
            maximum: 5
```

E.4 MSAG Conversion Service

E.4.1 OpenAPI Interface Description

```
openapi: 3.0.1
info:
  title: MSAG Conversion Service
  version: "1.0"
servers:
  - url: http://localhost/Mcs/v1
paths:
  /PidfloToMsag:
    post:
      tags:
        - PIDFLOtoMSAGConversion
      summary: Converts PIDF-LO to MSAG data
      operationId: PIDFLOtoMSAGConversion
      requestBody:
        description: PIDF-LO data
        content:
          application/json:
            schema:
              type: string
        required: true
      responses:
        '200':
          description: Data successfully converted
          content:
            application/xml:
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
            schema:
              $ref: '#/components/schemas/MsagData'
        '307':
          description: Temporary Redirect
          headers:
            Location:
              description: Referral URI of another MCS
              schema:
                type: string
                format: uri
        '454':
          description: Unspecified Error
        '468':
          description: No Address Found
        '469':
          description: Unknown MCS/GCS
  /MsagToPidfLo:
    post:
      tags:
        - MSAGtoPIDFLOConversion
      summary: Converts MSAG to PIDF-LO data
      operationId: MSAGtoPIDFLOConversion
      requestBody:
        description: MSAG data
        content:
          application/json:
            schema:
              type: string
        required: true
      responses:
        '200':
          description: Data successfully converted
          content:
            application/xml:
              schema:
                $ref: '#/components/schemas/PidfLoData'
        '307':
          description: Temporary Redirect
          headers:
            Location:
              description: Referral URI of another MCS
              schema:
                type: string
                format: uri
        '454':
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
          description: Unspecified Error
        '468':
          description: No Address Found
        '469':
          description: Unknown MCS/GCS
  /Versions:
    servers:
      - url: https://api.example.com/Mcs
        description: Override base path for Versions query
    get:
      tags:
        - RetrieveVersions
      summary: Retrieves all supported versions, vendor parameter is
optional.
      operationId: RetrieveVersions
      responses:
        '200':
          description: Versions found
          content:
            application/json:
              schema:
                $ref: 'i3-common.yaml#/components/schemas/VersionsArray'
components:
  schemas:
    PidfLoData:
      type: object
      required:
        - pidfLoAddress
      properties:
        pidfLoAddress:
          type: string
    MsagData:
      type: object
      required:
        - msagAddress
      properties:
        msagAddress:
          type: string
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

E.4.2 Examples

E.5 Geocode Conversion Service

E.5.1 OpenAPI Interface Description

```
openapi: 3.0.1
info:
  title: Geocode Conversion Service
  version: "1.0"
servers:
  - url: http://localhost/Gcs/v1
paths:
  /Geocode:
    post:
      tags:
        - GeocodeRequest
      summary: Converts civic address to geodetic representation of the
location in PIDF-LO format
      operationId: GeocodeRequest
      requestBody:
        description: PIDF-LO data
        content:
          application/json:
            schema:
              type: string
        required: true
      responses:
        '200':
          description: Data successfully converted
          content:
            application/xml:
              schema:
                $ref: '#/components/schemas/GeodeticData'
        '307':
          description: Temporary Redirect
          headers:
            Location:
              description: Referral URI of another GCS
              schema:
                type: string
                format: uri
        '454':
          description: Unspecified Error
        '468':
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
          description: No Address Found
        '469':
          description: Unknown MCS/GCS
  /ReverseGeocode:
    post:
      tags:
        - ReverseGeocodeRequest
      summary: Converts geodetic representation of the location to civic
address in PIDF-LO format
      operationId: ReverseGeocodeRequest
      requestBody:
        description: PIDF-LO data
        content:
          application/json:
            schema:
              type: string
        required: true
      responses:
        '200':
          description: Data successfully converted
          content:
            application/xml:
              schema:
                $ref: '#/components/schemas/CivicAddress'
        '307':
          description: Temporary Redirect
          headers:
            Location:
              description: Referral URI of another GCS
              schema:
                type: string
                format: uri
        '468':
          description: No Address Found
        '469':
          description: Unknown MCS/GCS
  /Versions:
    servers:
      - url: https://api.example.com/Gcs
        description: Override base path for Versions query
    get:
      tags:
        - RetrieveVersions
      summary: Retrieves all supported versions, vendor parameter is
optional.
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
      operationId: RetrieveVersions
      responses:
        '200':
          description: Versions found
          content:
            application/json:
              schema:
                $ref: 'i3-common.yaml#/components/schemas/VersionsArray'
components:
  schemas:
    GeodeticData:
      type: object
      required:
        - pidfLoGeo
      properties:
        pidfLoGeo:
          type: string
    CivicAddress:
      type: object
      required:
        - pidfLoAddress
      properties:
        pidfLoAddress:
          type: string
```

E.5.2 Examples

E.6 Test Call

E.6.1 OpenAPI Interface Description

```
openapi: 3.0.1
info:
  title: Test Call Service
  version: "1.0"
servers:
  - url: http://localhost/TestCall/v1
paths:
  /SendCallRequests/{psapId}:
    put:
      tags:
        - SendCallRequests
      summary: Updates an existing send call request identified by the
PSAP ID or creates a new one if the request does not exist
      operationId: SendCallRequests
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
      parameters:
        - name: psapId
          in: path
          description: ID of the PSAP which wishes to have test calls sent
to it
          required: true
          schema:
            type: string
      requestBody:
        description: Request to update/create
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/SendCallRequests'
        required: true
      responses:
        '200':
          description: Request successfully updated/created
        '442':
          description: Unacceptable Parameters
        '454':
          description: Unspecified Error
        '458':
          description: Policy violation
  /Versions:
    servers:
      - url: https://api.example.com/TestCall
        description: Override base path for Versions query
    get:
      tags:
        - RetrieveVersions
      summary: Retrieves all supported versions, vendor parameter is
optional.
      operationId: RetrieveVersions
      responses:
        '200':
          description: Versions found
          content:
            application/json:
              schema:
                $ref: 'i3-common.yaml#/components/schemas/VersionsArray'
components:
  schemas:
    SendCallRequests:
      type: object
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
      required:
        - psapId
        - location
        - frequency
        - discrepancyRateLimit
        - startDate
        - endDate
      properties:
        psapId:
          type: string
          readOnly: true
        location:
          type: string
        frequency:
          type: integer
          format: int32
        discrepancyRateLimit:
          type: integer
          format: int32
        startDate:
          type: string
          format: date-time
          example: '2020-03-10T10:00:00-05:00'
        endDate:
          type: string
          format: date-time
          example: '2020-03-11T10:00:00-05:00'
        testConditions:
          $ref: '#/components/schemas/PrrTest'
    PrrTest:
      type: object
      required:
        - hostName
        - nominalNextHop
        - conditions
      properties:
        hostName:
          type: string
          description: ESRP Hostname that test conditions are specified
for.
        nominalNextHop:
          type: string
          format: uri
          description: URI of for nominal next hop that rule set
conditions are applied to.
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
        conditions:
          type: array
          items:
            type: object
            required:
              - name
              - value
            properties:
              name:
                $ref: 'i3-common.yaml#/components/schemas/ConditionType'
                description: Condition name
              value:
                type: string
                description: Condition value
```

E.6.2 Examples

E.7 Additional Data Repository

E.7.1 OpenAPI Interface Description

```
openapi: 3.0.1
info:
  title: IS-ADR Service
  version: "1.0"
servers:
  - url: http://localhost/Adr/v1
paths:
  /AdditionalData:
    get:
      tags:
        - RetrieveCallerAdditionalData
      summary: Retrieves Additional Data of the caller in XML format or a
reference to the Additional Data. Provides ADR search capability by
identity (Identity-Searchable).
      operationId: RetrieveCallerAdditionalData
      parameters:
        - name: callerUri
          in: query
          description: Caller URI (taken from From or PAI)
          required: true
          schema:
            type: string
      responses:
        '200':
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
            description: Additional Data found
            content:
              application/xml:
                schema:
                  $ref: '#/components/schemas/AdditionalDataValue'
              application/json:
                schema:
                  $ref: '#/components/schemas/AdditionalDataReference'
          '307':
            description: Temporary Redirect
            headers:
              Location:
                description: Referral URI of ADR
                schema:
                  type: string
                  format: uri
          '404':
            description: Not found
          '454':
            description: Unspecified Error
  /Versions:
    servers:
      - url: https://api.example.com/Adr
        description: Override base path for Versions query
    get:
      tags:
        - RetrieveVersions
      summary: Retrieves all supported versions, vendor parameter is
optional.
      operationId: RetrieveVersions
      responses:
        '200':
          description: Versions found
          content:
            application/json:
              schema:
                $ref: 'i3-common.yaml#/components/schemas/VersionsArray'
components:
  schemas:
    AdditionalDataValue:
      type: string
    AdditionalDataReference:
      type: string
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

E.7.2 Examples

E.8 Logging Service

E.8.1 OpenAPI Interface Description

```
openapi: 3.0.1
info:
  title: Logging Service
  version: "1.0"
servers:
  - url: https://api.example.com/Logging/v1
paths:
  /LogEvents:
    get:
      tags:
        - RetrieveLogEvents, ListLogEventsByEventTypeAndDateRange
      summary: Retrieves LogEvents. Use limit and start parameters for
pagination.
      operationId: RetrieveLogEvents
      parameters:
        - name: limit
          in: query
          description: Maximum number of results to return
          required: false
          schema:
            type: integer
            format: int32
        - name: start
          in: query
          description: First item in the page of results, as an ordinal 1-
based integer
          required: false
          schema:
            type: integer
            format: int32
            minimum: 1
        - name: logEventType
          in: query
          description: LogEvent type
          required: false
          schema:
            $ref: '#/components/schemas/LogEventType'
        - name: startTime
          in: query
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
          description: Start time
          required: false
          schema:
            type: string
            format: date-time
            example: '2020-03-10T11:00:01-05:00'
        - name: endTime
          in: query
          description: End time
          required: false
          schema:
            type: string
            format: date-time
            example: '2020-03-15T11:00:01-05:00'
      responses:
        '200':
          description: LogEvents found
          content:
            application/json:
              schema:
                $ref: '#/components/schemas/LogEventContainerArray'
        '404':
          description: Not found
    post:
      tags:
        - LogEvent
      summary: Logs a new event into the Logging Service
      operationId: LogEvent
      requestBody:
        description: LogEvent data to add (JWS using flattened JSON
serialization)
        content:
          application/json:
            schema:
              $ref: 'i3-common.yaml#/components/schemas/Jws'
        required: true
      responses:
        '201':
          description: LogEvent successfully logged
          content:
            application/json:
              schema:
                type: string
                description: logEventId of the new logEvent
        '434':
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
          description: Signature Verification Failure
        '438':
          description: Unacceptable Algorithm
        '454':
          description: Unspecified Error
        '460':
          description: Bad LogEvent
        '461':
          description: LogEvent too big
        '462':
          description: LogEvent extension not on approved list
        '463':
          description: LogEvent extension on disallowed list
  /LogEvents/{logEventId}:
    get:
      tags:
        - RetrieveLogEvent
      summary: Retrieves a LogEvent based on logEventId. LogEvent is
returned in JWS using flattened JSON serialization
      operationId: RetrieveLogEvent
      parameters:
        - name: logEventId
          in: path
          description: ID of the logEvent
          required: true
          schema:
            type: string
      responses:
        '200':
          description: LogEvent found
          content:
            application/json:
              schema:
                $ref: 'i3-common.yaml#/components/schemas/Jws'
        '404':
          description: Not found
  /Conversations:
    get:
      tags:
        - RetrieveConversationText
      summary: Returns an HTML formatted record suitable for human
consumption of the text portion of a call, including all text sent by all
parties.
      operationId: RetrieveConversationText
      parameters:
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
        - name: callId
          in: query
          description: Call ID of the call
          required: true
          schema:
            type: string
      responses:
        '200':
          description: Conversation found
          content:
            application/json:
              schema:
                type: string
        '404':
          description: Not found
        '454':
          description: Unspecified Error
        '464':
          description: No Text in this Call
  /LogEventIds:
    get:
      tags:
        - ListLogEventsByCallId, ListLogEventsByIncidentId
      summary: Retrieves LogEvents IDs. Use limit and start parameters for
pagination.
      operationId: ListLogEventsById
      parameters:
        - name: limit
          in: query
          description: Maximum number of results to return
          required: false
          schema:
            type: integer
            format: int32
        - name: start
          in: query
          description: First item in the page of results, as an ordinal 1-
based integer
          required: false
          schema:
            type: integer
            format: int32
            minimum: 1
        - name: callId
          in: query
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
          description: Call ID of the call
          required: false
          schema:
            type: string
        - name: incidentId
          in: query
          description: Incident ID of the call
          required: false
          schema:
            type: string
      responses:
        '200':
          description: LogEvents found
          content:
            application/json:
              schema:
                $ref: '#/components/schemas/LogEventIdArray'
        '404':
          description: Not found
        '454':
          description: Unspecified Error
  /CallIds:
    get:
      tags:
        - ListCallsByIncidentId, ListCallsByDateRange, ListCallsByLocation
      summary: Returns a list of Call Identifiers associated with a
specific Incident Tracking Identifier, occurred within a time range or
within a specified geographic region.
      operationId: ListCalls
      parameters:
        - name: limit
          in: query
          description: Maximum number of results to return
          required: false
          schema:
            type: integer
            format: int32
        - name: start
          in: query
          description: First item in the page of results, as an ordinal 1-
based integer
          required: false
          schema:
            type: integer
            format: int32
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
        minimum: 1
    - name: incidentId
      in: query
      description: Incident ID of the call
      required: false
      schema:
        type: string
    - name: startTime
      in: query
      description: Start time
      required: false
      schema:
        type: string
        format: date-time
        example: '2020-03-10T11:00:01-05:00'
    - name: endTime
      in: query
      description: End time
      required: false
      schema:
        type: string
        format: date-time
        example: '2020-03-15T11:00:01-05:00'
    - name: area
      in: query
      description: Area of interest
      required: false
      schema:
        type: string
  responses:
    '200':
      description: Calls found
      content:
        application/json:
          schema:
            $ref: '#/components/schemas/CallIdArray'
    '404':
      description: Not found
    '454':
      description: Unspecified Error
    '465':
      description: Bad Timestamp
    '466':
      description: endTime occurs before startTime
    '467':
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
          description: Bad Geoshape
  /IncidentIds:
    get:
      tags:
        - ListIncidentsByDateRange, ListIncidentsByLocation
      summary: Returns a list of Incident Tracking Identifiers occurring
within a time/date range. Returns a list of Incidents that occurred within
a specified geographic region.
      operationId: ListIncidents
      parameters:
        - name: limit
          in: query
          description: Maximum number of results to return
          required: false
          schema:
            type: integer
            format: int32
        - name: start
          in: query
          description: First item in the page of results, as an ordinal 1-
based integer
          required: false
          schema:
            type: integer
            format: int32
            minimum: 1
        - name: startTime
          in: query
          description: Start time
          required: false
          schema:
            type: string
            format: date-time
            example: '2020-03-10T11:00:01-05:00'
        - name: endTime
          in: query
          description: End time
          required: false
          schema:
            type: string
            format: date-time
            example: '2020-03-15T11:00:01-05:00'
        - name: area
          in: query
          description: Area of interest
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
          required: false
          schema:
            type: string
      responses:
        '200':
          description: Incidents found
          content:
            application/json:
              schema:
                $ref: '#/components/schemas/IncidentIdArray'
        '404':
          description: Not found
        '454':
          description: Unspecified Error
        '465':
          description: Bad Timestamp
        '466':
          description: endTime occurs before startTime
        '467':
          description: Bad Geoshape
  /AgencyIds:
    get:
      tags:
        - ListAgenciesByCallId, ListAgenciesByIncidentId
      summary: Returns a list of agencies involved in a Call or an
Incident.
      operationId: ListAgenciesById
      parameters:
        - name: limit
          in: query
          description: Maximum number of results to return
          required: false
          schema:
            type: integer
            format: int32
        - name: start
          in: query
          description: First item in the page of results, as an ordinal 1-
based integer
          required: false
          schema:
            type: integer
            format: int32
            minimum: 1
        - name: incidentId
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
            in: query
            description: Incident ID of the call
            required: false
            schema:
              type: string
          - name: callId
            in: query
            description: Incident ID of the call
            required: false
            schema:
              type: string
        responses:
          '200':
            description: Agencies found
            content:
              application/json:
                schema:
                  $ref: '#/components/schemas/AgencyIdArray'
          '404':
            description: Not found
          '454':
            description: Unspecified Error
    /Versions:
      servers:
        - url: https://api.example.com/Logging
          description: Override base path for Versions query
      get:
        tags:
          - RetrieveVersions
        summary: Retrieves all supported versions, vendor parameter is
optional.
        operationId: RetrieveVersions
        responses:
          '200':
            description: Versions found
            content:
              application/json:
                schema:
                  $ref: 'i3-common.yaml#/components/schemas/VersionsArray'
components:
  schemas:
    LogEventContainerArray:
      type: object
      required:
        - count
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
      - totalCount
      - logEventContainers
    properties:
      count:
        type: integer
        format: int32
        description: Number of items in the array
      totalCount:
        type: integer
        format: int32
        description: Total number of items found
      logEventContainers:
        type: array
        items:
          $ref: '#/components/schemas/LogEventContainer'
        description: Array of LogEvent Container objects
  LogEventContainer:
    type: object
    required:
      - logEventId
      - logEvent
    properties:
      logEventId:
        type: string
        readOnly: true
      rtsp:
        type: array
        items:
          type: string
      logEvent:
        $ref: 'i3-common.yaml#/components/schemas/Jws'
  LogEventIdArray:
    type: object
    required:
      - count
      - totalCount
      - logEventIds
    properties:
      count:
        type: integer
        format: int32
        description: Number of items in the array
      totalCount:
        type: integer
        format: int32
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
        description: Total number of items found
      logEventIds:
        type: array
        items:
          type: string
        description: Array of LogEvent IDs
CallIdArray:
  type: object
  required:
    - count
    - totalCount
    - callIds
  properties:
    count:
      type: integer
      format: int32
      description: Number of items in the array
    totalCount:
      type: integer
      format: int32
      description: Total number of items found
    callIds:
      type: array
      items:
        type: string
      description: Array of Call IDs
IncidentIdArray:
  type: object
  required:
    - count
    - totalCount
    - incidentIds
  properties:
    count:
      type: integer
      format: int32
      description: Number of items in the array
    totalCount:
      type: integer
      format: int32
      description: Total number of items found
    logEventIds:
      type: array
      items:
        type: string
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
          description: Array of Incident IDs
      AgencyIdArray:
        type: object
        required:
          - count
          - totalCount
          - agencyIds
        properties:
          count:
            type: integer
            format: int32
            description: Number of items in the array
          totalCount:
            type: integer
            format: int32
            description: Total number of items found
          agencyIds:
            type: array
            items:
              type: string
            description: Array of Agency IDs
      LogEventType:
        type: string
        enum: [CallProcessLogEvent, CallStartLogEvent, CallEndLogEvent,
RecCallStartLogEvent, RecCallEndLogEvent, CallTransferLogEvent,
RouteLogEvent, MediaStartLogEvent, MediaEndLogEvent,
RecMediaStartLogEvent, RecMediaEndLogEvent,
               RecordingFailedLogEvent, MessageLogEvent,
AdditionalAgencyLogEvent, IncidentMergeLogEvent, IncidentUnMergeLogEvent,
IncidentLinkLogEvent, IncidentUnLinkLogEvent, IncidentClearLogEvent,
IncidentReopenLogEvent, LostQueryLogEvent,
               LostResponseLogEvent, CallSignalingMessageLogEvent,
SipRecMetadataLogEvent, NonRtpMediaMessageLogEvent,
AliLocationQueryLogEvent, AliLocationResponseLogEvent,
MalformedMessageLogEvent, IncidentSplitLogEvent, EidoLogEvent,
               DiscrepancyReportLogEvent, ElementStateChangeLogEvent,
ServiceStateChangeLogEvent, AdditionalDataQueryLogEvent,
AdditionalDataResponseLogEvent, LocationQueryLogEvent,
LocationResponseLogEvent, CallStateChangeLogEvent,
               GatewayCallLogEvent, HookflashLogEvent, LegacyDigitsLogEvent,
AgentStateChangeLogEvent, QueueStateChangeLogEvent,
KeepAliveFailureLogEvent, RouteRuleMsgLogEvent, PolicyChangeLogEvent,
               VersionsLogEvent, SubscribeLogEvent]
      LogEvent:
        type: object
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
    required:
      - logEventType
      - timestamp
      - agencyId
      - elementId
    properties:
      clientAssignedIdentifier:
        type: string
      logEventType:
        $ref: '#/components/schemas/LogEventType'
      timestamp:
        type: string
        format: date-time
        example: '2020-03-10T11:00:01-05:00'
      elementId:
        type: string
      agencyId:
        type: string
      agencyAgentId:
        type: string
      agencyPositionId:
        type: string
      callId:
        type: string
      incidentId:
        type: string
      callIdSip:
        type: string
      ipAddressPort:
        type: string
      extension:
        type: object
    discriminator:
      propertyName: logEventType
  CallProcessLogEvent:
    allOf:
      - $ref: '#/components/schemas/LogEvent'
  CallStartLogEvent:
    allOf:
      - $ref: '#/components/schemas/LogEvent'
      - $ref: '#/components/schemas/CallLogEvent'
  CallEndLogEvent:
    allOf:
      - $ref: '#/components/schemas/LogEvent'
      - $ref: '#/components/schemas/CallLogEvent'
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
    RecCallStartLogEvent:
      allOf:
        - $ref: '#/components/schemas/LogEvent'
        - $ref: '#/components/schemas/CallLogEvent'
    RecCallEndLogEvent:
      allOf:
        - $ref: '#/components/schemas/LogEvent'
        - $ref: '#/components/schemas/CallLogEvent'
    CallTransferLogEvent:
      allOf:
        - $ref: '#/components/schemas/LogEvent'
        - type: object
          required:
            - target
            - targetCallIdSip
          properties:
            target:
              type: string
              format: uri
            targetCallIdSip:
              type: string
    RouteLogEvent:
      allOf:
        - $ref: '#/components/schemas/LogEvent'
        - type: object
          required:
            - recipientUri
            - ruleId
            - policyOwner
            - policyType
          properties:
            recipientUri:
              type: string
              format: uri
            ruleId:
              type: string
            policyOwner:
              type: string
            policyType:
              type: string
              description: Values limited to those in the policyType
registry
            policyQueueName:
              type: string
              format: uri
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
        policyId:
          type: string
        cause:
          type: string
MediaStartLogEvent:
  allOf:
    - $ref: '#/components/schemas/LogEvent'
    - type: object
      required:
        - sdp
        - mediaLabal
        - direction
      properties:
        sdp:
          type: string
        mediaLabel:
          type: array
          items:
              type: string
        direction:
          $ref: '#/components/schemas/Direction'
MediaEndLogEvent:
  allOf:
    - $ref: '#/components/schemas/LogEvent'
    - type: object
      required:
        - mediaLabel
      properties:
        mediaLabel:
          type: array
          items:
            type: string
        mediaQualityStats:
          type: string
RecMediaStartLogEvent:
  allOf:
    - $ref: '#/components/schemas/LogEvent'
    - type: object
      required:
        - sdp
        - mediaLabel
      properties:
        sdp:
          type: string
        mediaLabel:
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
              type: array
              items:
                type: string
            direction:
              $ref: '#/components/schemas/Direction'
            mediaTranscodeFrom:
              type: string
    RecMediaEndLogEvent:
      allOf:
        - $ref: '#/components/schemas/LogEvent'
        - type: object
          required:
            - mediaLabel
          properties:
            mediaLabel:
              type: array
              items:
                type: string
            mediaQualityStats:
              type: string
            mediaTranscodeFrom:
              type: string
    RecordingFailedLogEvent:
      allOf:
        - $ref: '#/components/schemas/LogEvent'
        - type: object
          required:
            - sdp
            - reasonCode
            - reasonText
          properties:
            sdp:
              type: string
            reasonCode:
              type: string
              description: Values limited to those in the ReasonCode
registry
            reasonText:
              type: string
    MessageLogEvent:
      allOf:
        - $ref: '#/components/schemas/LogEvent'
        - type: object
          required:
            - text
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
        - direction
      properties:
        text:
          type: string
        direction:
          $ref: '#/components/schemas/Direction'
AdditionalAgencyLogEvent:
  allOf:
    - $ref: '#/components/schemas/LogEvent'
    - type: object
      required:
        - agencyId
      properties:
        agencyId:
          type: string
IncidentMergeLogEvent:
  allOf:
    - $ref: '#/components/schemas/LogEvent'
    - type: object
      required:
        - mergeIncidentId
      properties:
        mergeIncidentId:
          type: string
IncidentUnMergeLogEvent:
  allOf:
    - $ref: '#/components/schemas/LogEvent'
    - type: object
      required:
        - unmergedFromIncidentId
      properties:
        unmergedFromIncidentId:
          type: string
IncidentLinkLogEvent:
  allOf:
    - $ref: '#/components/schemas/LogEvent'
    - type: object
      required:
        - linkedIncidentId
        - relationship
      properties:
        linkedIncidentId:
          type: string
        relationship:
          type: string
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
          enum: [parent, child, unspecified]
IncidentUnLinkLogEvent:
  allOf:
    - $ref: '#/components/schemas/LogEvent'
    - type: object
      required:
        - unlinkedFromIncidentId
      properties:
        unlinkedFromIncidentId:
          type: string
IncidentClearLogEvent:
  allOf:
    - $ref: '#/components/schemas/LogEvent'
IncidentReopenLogEvent:
  allOf:
    - $ref: '#/components/schemas/LogEvent'
LostQueryLogEvent:
  allOf:
    - $ref: '#/components/schemas/LogEvent'
    - type: object
      required:
        - queryAdapter
        - direction
        - queryId
      properties:
        queryAdapter:
          type: string
        direction:
          $ref: '#/components/schemas/Direction'
        queryId:
          type: string
        malformedQuery:
          type: string
LostResponseLogEvent:
  allOf:
    - $ref: '#/components/schemas/LogEvent'
    - type: object
      required:
        - responseAdapter
        - direction
        - responseId
      properties:
        responseAdapter:
          type: string
        direction:
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
          $ref: '#/components/schemas/Direction'
        responseStatus:
          type: string
        responseId:
          type: string
        malformedResponse:
          type: string
CallSignalingMessageLogEvent:
  allOf:
    - $ref: '#/components/schemas/LogEvent'
    - type: object
      required:
        - text
        - direction
      properties:
        text:
          type: string
        direction:
          $ref: '#/components/schemas/Direction'
        protocol:
          type: string
SipRecMetadataLogEvent:
  allOf:
    - $ref: '#/components/schemas/LogEvent'
    - type: object
      required:
        - text
      properties:
        text:
          type: string
NonRtpMediaMessageLogEvent:
  allOf:
    - $ref: '#/components/schemas/LogEvent'
    - type: object
      required:
        - text
        - direction
      properties:
        text:
          type: string
        direction:
          $ref: '#/components/schemas/Direction'
        protocol:
          type: string
AliLocationQueryLogEvent:
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
      allOf:
        - $ref: '#/components/schemas/LogEvent'
        - type: object
          required:
            - text
            - direction
            - queryId
          properties:
            text:
              type: string
            direction:
              $ref: '#/components/schemas/Direction'
            queryId:
              type: string
    AliLocationResponseLogEvent:
      allOf:
        - $ref: '#/components/schemas/LogEvent'
        - type: object
          required:
            - text
            - direction
            - responseId
          properties:
            text:
              type: string
            direction:
              $ref: '#/components/schemas/Direction'
            responseStatus:
              type: string
              description: Values limited to those in the Status Codes
registry
            responseId:
              type: string
    MalformedMessageLogEvent:
      allOf:
        - $ref: '#/components/schemas/LogEvent'
        - type: object
          required:
            - text
            - ipAddress
          properties:
            text:
              type: string
            ipAddress:
              type: string
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
        explanationText:
          type: string
IncidentSplitLogEvent:
  allOf:
    - $ref: '#/components/schemas/LogEvent'
    - type: object
      required:
        - incidentId
        - type
      properties:
        incidentId:
          type: string
        type:
          type: string
          enum: [old, new]
EidoLogEvent:
  allOf:
    - $ref: '#/components/schemas/LogEvent'
    - type: object
      required:
        - direction
      properties:
        body:
          type: string
        reference:
          type: string
        direction:
          $ref: '#/components/schemas/Direction'
DiscrepancyReportLogEvent:
  allOf:
    - $ref: '#/components/schemas/LogEvent'
    - type: object
      required:
        - contents
        - direction
        - type
      properties:
        contents:
          type: string
        direction:
          $ref: '#/components/schemas/Direction'
        type:
          type: string
ElementStateChangeLogEvent:
  allOf:
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
      - $ref: '#/components/schemas/LogEvent'
      - type: object
        required:
          - notificationContents
          - direction
        properties:
          notificationContents:
            type: string
          StateChangeNotificationContents:
            type: string
          affectedElementId:
            type: string
          direction:
            $ref: '#/components/schemas/Direction'
  ServiceStateChangeLogEvent:
    allOf:
      - $ref: '#/components/schemas/LogEvent'
      - type: object
        required:
          - newState
          - affectedServiceIdentifier
          - direction
        properties:
          newState:
            type: string
          newSecurityPosture:
            type: string
          affectedServiceIdentifier:
            type: string
          direction:
            $ref: '#/components/schemas/Direction'
  AdditionalDataQueryLogEvent:
    allOf:
      - $ref: '#/components/schemas/LogEvent'
      - type: object
        required:
          - uri
          - text
          - direction
          - queryId
        properties:
          uri:
            type: string
            format: uri
          text:
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
              type: string
            direction:
              $ref: '#/components/schemas/Direction'
            queryId:
              type: string
    AdditionalDataResponseLogEvent:
      allOf:
        - $ref: '#/components/schemas/LogEvent'
        - type: object
          required:
            - text
            - direction
            - responseId
          properties:
            text:
              type: string
            direction:
              $ref: '#/components/schemas/Direction'
            responseStatus:
              type: string
              description: Values limited to those in the Status Codes
registry
            responseId:
              type: string
    LocationQueryLogEvent:
      allOf:
        - $ref: '#/components/schemas/LogEvent'
        - type: object
          required:
            - uri
            - text
            - direction
            - queryId
          properties:
            uri:
              type: string
              format: uri
            text:
              type: string
            direction:
              $ref: '#/components/schemas/Direction'
            queryId:
              type: string
    LocationResponseLogEvent:
      allOf:
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
        - $ref: '#/components/schemas/LogEvent'
        - type: object
          required:
            - text
            - direction
            - responseId
          properties:
            text:
              type: string
            direction:
              $ref: '#/components/schemas/Direction'
            responseStatus:
              type: string
              description: Values limited to those in the Status Codes
registry
            responseId:
              type: string
    CallStateChangeLogEvent:
      allOf:
        - $ref: '#/components/schemas/LogEvent'
        - type: object
          required:
            - state
            - direction
            - legCallId
          properties:
            state:
              type: string
              description: Values limited to those in the CallStates
registry
            direction:
              $ref: '#/components/schemas/Direction'
            legCallId:
              type: string
            targetId:
              type: string
            changeReason:
              type: string
    GatewayCallLogEvent:
      allOf:
        - $ref: '#/components/schemas/LogEvent'
        - type: object
          properties:
            portTrunkGroup:
              type: string
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
        pAni:
          type: string
        digits:
          type: string
        direction:
          $ref: '#/components/schemas/Direction'
        signallingProtocol:
          type: string
        legacyCallId:
          type: string
HookflashLogEvent:
  allOf:
    - $ref: '#/components/schemas/LogEvent'
    - type: object
      properties:
        lineId:
          type: string
LegacyDigitsLogEvent:
  allOf:
    - $ref: '#/components/schemas/LogEvent'
    - type: object
      required:
        - digits
        - sentReceived
        - type
      properties:
        digits:
          type: string
        sentReceived:
          type: string
          enum: [sent, received]
        type:
          type: string
          enum: [DTMF, MF]
AgentStateChangeLogEvent:
  allOf:
    - $ref: '#/components/schemas/LogEvent'
    - type: object
      required:
        - primaryAgentState
      properties:
        primaryAgentState:
          type: string
          enum: [Available, NotAvailable]
        secondaryAgentState:
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
              type: string
              description: Values limited to those in the Secondary Agent
State registry
            deviceId:
              type: string
    QueueStateChangeLogEvent:
      allOf:
        - $ref: '#/components/schemas/LogEvent'
        - type: object
          required:
            - notificationContents
            - queueId
            - direction
          properties:
            notificationContents:
              type: string
            queueId:
              type: string
            direction:
              $ref: '#/components/schemas/Direction'
    KeepAliveFailureLogEvent:
      allOf:
        - $ref: '#/components/schemas/LogEvent'
        - type: object
          required:
            - responseStatus
          properties:
            responseStatus:
              type: string
              description: Values limited to those in the Status Codes
registry
    RouteRuleMsgLogEvent:
      allOf:
        - $ref: '#/components/schemas/LogEvent'
        - type: object
          required:
            - ruleId
            - priority
            - message
            - policyOwner
            - policyType
          properties:
            ruleId:
              type: string
            priority:
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
              type: integer
              format: int32
            message:
              type: string
            policyOwner:
              type: string
            policyType:
              type: string
              description: Values limited to those in the policyType
registry
            policyQueueName:
              type: string
              format: uri
            policyId:
              type: string
    PolicyChangeLogEvent:
      allOf:
        - $ref: '#/components/schemas/LogEvent'
        - type: object
          required:
            - policyType
            - owner
            - changeType
            - policyContent
            - policyStoreId
            - policyEditor
          properties:
            policyType:
              type: string
              description: Values limited to those in the policyType
registry
            owner:
              type: string
            changeType:
              type: string
              enum: [CREATE, UPDATE, DELETE]
            policyContent:
              type: string
            policyStoreId:
              type: string
            policyEditor:
              type: string
            policyQueueName:
              type: string
              format: uri
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
            policyId:
              type: string
    VersionsLogEvent:
      allOf:
        - $ref: '#/components/schemas/LogEvent'
        - type: object
          required:
            - source
            - response
          properties:
            source:
              type: string
            response:
              type: string
    SubscribeLogEvent:
      allOf:
        - $ref: '#/components/schemas/LogEvent'
        - type: object
          required:
            - package
            - peer
            - parameter
            - expiration
            - response
            - purpose
            - direction
            - subscriptionId
          properties:
            package:
              type: string
              description: Values limited to those in the Event Package
registry
            peer:
              type: string
            parameter:
              type: array
              items:
                type: object
                properties:
                  type:
                    type: string
                  value:
                    type: string
            expiration:
              type: integer
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
              format: int32
            response:
              type: string
            purpose:
              type: string
              enum: [initial, refresh, terminate]
            direction:
              $ref: '#/components/schemas/Direction'
            subscriptionId:
              type: string
    CallLogEvent:
      type: object
      required:
        - direction
      properties:
        direction:
          $ref: '#/components/schemas/Direction'
        standardPrimaryCallType:
          type: string
          description: Values limited to those in the LogEvent CallTypes
registry
        standardSecondaryCallType:
          type: string
          description: Values limited to those in the LogEvent CallTypes
registry
        localCallType:
          type: string
        localUse:
          type: object
        to:
          type: string
        from:
          type: string
    Direction:
      type: string
      enum: [incoming, outgoing]
```

E.8.2 Examples

E.9 Bad Actor Service

E.9.1 OpenAPI Interface Description

```
openapi: 3.0.1
info:
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
  title: Bad Actor Service
  version: "1.0"
servers:
  - url: http://localhost/BadActor/v1
paths:
  /BadActors:
    post:
      tags:
        - BadActorRequest
      summary: Identifies a source as a "Bad Actor"
      operationId: BadActorRequest
      requestBody:
        description: Bad actor source Id
        content:
          application/json:
            schema:
              type: string
        required: true
      responses:
        '201':
          description: Bad Actor successfully added
        '401':
          description: Unauthorized
        '432':
          description: Already reported
        '433':
          description: No such sourceId
        '454':
          description: Unspecified Error
  /Versions:
    servers:
      - url: https://api.example.com/BadActor
        description: Override base path for Versions query
    get:
      tags:
        - RetrieveVersions
      summary: Retrieves all supported versions, vendor parameter is
optional.
      operationId: RetrieveVersions
      responses:
        '200':
          description: Versions found
          content:
            application/json:
              schema:
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
                $ref: 'i3-common.yaml#/components/schemas/VersionsArray'
```

E.10 Service/Agency Locator Service

E.10.1 OpenAPI Interface Description

```
openapi: 3.0.1
info:
  title: Service/Agency Locator
  version: "1.0"
servers:
  - url: http://localhost/ServiceAgencyLocator/v1
paths:
  /LocatorRecordUris:
    get:
      tags:
        - SearchByName
      summary: Retrieves Service/Agency Locator Records URIs
      operationId: SearchByName
      parameters:
        - name: limit
          in: query
          description: Maximum number of results to return
          required: false
          schema:
            type: integer
            format: int32
        - name: start
          in: query
          description: First item in the page of results, as an ordinal 1-
based integer
          required: false
          schema:
            type: integer
            format: int32
            minimum: 1
        - name: serviceAgencyName
          in: query
          description: Name of the Service or Agency, wildcards can be
used
          required: true
          schema:
            type: string
      responses:
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
        '200':
          description: URIs found
          content:
            application/json:
              schema:
                $ref: '#/components/schemas/LocatorRecordUriArray'
        '404':
          description: Not found
        '454':
          description: Unspecified Error
  /NameSets:
    get:
      tags:
        - InterESInetSearchIndex
      summary: Retrieves Service/Agency names the Locator is aware of
      operationId: InterESInetSearchIndex
      parameters:
        - name: limit
          in: query
          description: Maximum number of results to return
          required: false
          schema:
            type: integer
            format: int32
        - name: start
          in: query
          description: First item in the page of results, as an ordinal 1-
based integer
          required: false
          schema:
            type: integer
            format: int32
            minimum: 1
      responses:
        '200':
          description: Namesets found
          content:
            application/json:
              schema:
                $ref: '#/components/schemas/NameSetArray'
        '404':
          description: Not found
        '441':
          description: Index beyond available names
        '454':
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
          description: Unspecified Error
  /Versions:
    servers:
      - url: https://api.example.com/ServiceAgencyLocator
        description: Override base path for Versions query
    get:
      tags:
        - RetrieveVersions
      summary: Retrieves all supported versions, vendor parameter is
optional.
      operationId: RetrieveVersions
      responses:
        '200':
          description: Versions found
          content:
            application/json:
              schema:
                $ref: 'i3-common.yaml#/components/schemas/VersionsArray'
components:
  schemas:
    LocatorRecordUriArray:
      type: object
      required:
        - count
        - totalCount
        - locatorUris
      properties:
        count:
          type: integer
          format: int32
          description: Number of items in the array
        totalCount:
          type: integer
          format: int32
          description: Total number of items found
        locatorUris:
          type: array
          items:
            $ref: '#/components/schemas/LocatorRecordUri'
          description: Array of Locator URI objects
    NameSetArray:
      type: object
      required:
        - count
        - totalCount
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
      - nameSets
    properties:
      count:
        type: integer
        format: int32
        description: Number of items in the array
      totalCount:
        type: integer
        format: int32
        description: Total number of items found
      nameSets:
        type: array
        items:
          $ref: '#/components/schemas/NameSet'
        description: Array of Name Sets objects
  LocatorRecordUri:
    type: object
    required:
      - locatorRecordUri
      - serviceAgencyName
      - uriType
    properties:
      uri:
        type: string
        format: uri
      serviceAgencyName:
        type: string
      uriType:
        type: string
        enum: [RecordUri, ReferralUri]
  LocatorRecord:
    type: object
    required:
      - recordId
      - serviceAgencyId
      - serviceAgencyName
      - serviceAgencyJcard
      - serviceAgencyTypes
      - loggerUri
    properties:
      recordId:
        type: string
      serviceAgencyId:
        type: string
      serviceAgencyName:
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
        type: string
      serviceAgencyJcard:
        type: string
      serviceAgencyTypes:
        type: array
        minItems: 1
        items:
          type: string
      emergencySipInterfaceUri:
        type: string
        format: uri
      adminLineUri:
        type: string
        format: uri
      loggerUri:
        type: string
        format: uri
      eidoInterfaceUri:
        type: string
        format: uri
      mdsFeatureInterfaceUri:
        type: string
        format: uri
      mdsImageInterfaceUri:
        type: string
        format: uri
      svcStateUri:
        type: string
        format: uri
      dscRptUri:
        type: string
        format: uri
      headJcard:
        type: string
      onDutySuperJcard:
        type: string
  NameSet:
    type: object
    properties:
      locatorUri:
        type: string
        format: uri
      names:
        type: array
        items:
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
                type: string
```

E.11 Notify Bodies

E.11.1 ESRP NOTIFY Notify Body

E.11.1.1 JSON Schema

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "version": "1.0",
  "title": "ESRP Notify NOTIFY",
  "description": "SIP NOTIFY message body for ESRP Notify notifications",
  "type": "object",
  "properties": {
    "esrpNotify": {
      "type": "object",
      "properties": {
        "queueUri": {
          "type": "string"
        },
        "eventCode": {
          "type": "string"
        },
        "urgency": {
          "type": "integer"
        },
        "comment": {
          "type": "string"
        },
        "callLocation": {
          "type": "string"
        },
        "additionalData": {
          "type": "string"
        },
        "esrpRule": {
          "type": "string"
        }
      },
      "required": [
        "queueUri",
        "eventCode",
        "urgency",
        "callLocation",
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
            "esrpRule"
          ]
        }
      },
      "required": [
        "esrpNotify"
      ]
    }
```

E.11.1.2 Gap-Overlap Notify Body

E.11.1.3 JSON Schema

```
    {
      "$schema": "http://json-schema.org/draft-04/schema#",
      "version": "1.0",
      "title": "Gap Overlap NOTIFY",
      "description": "SIP NOTIFY message body for Gap Overlap notifications",
      "type": "object",
      "properties": {
        "gapOverlap": {
          "type": "object",
          "properties": {
            "agencies": {
              "type": "array",
              "items": {
                "type": "string"
              }
            },
            "layers": {
              "type": "array",
              "items": {
                "type": "string"
              }
            },
            "gap": {
              "type": "boolean"
            },
            "dateTime": {
              "type": "string"
            },
            "area": {
              "type": "string"
            }
          },
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
        "required": [
          "agencies",
          "layers",
          "gap",
          "dateTime",
          "area"
        ]
      }
    },
    "required": [
      "gapOverlap"
    ]
  }
```

E.11.2 Abandoned Call Notify Body

E.11.2.1 JSON Schema

```
  {
    "$schema": "http://json-schema.org/draft-04/schema#",
    "version": "1.0",
    "title": "Abandoned Call NOTIFY",
    "description": "SIP NOTIFY message body for Abandoned Call
  notifications",
    "type": "object",
    "properties": {
      "abandonedCall": {
        "type": "object",
        "properties": {
          "invite": {
            "type": "string"
          },
          "inviteTimestamp": {
            "type": "string"
          },
          "cancelTimestamp": {
            "type": "string"
          }
        },
        "required": [
          "invite",
          "inviteTimestamp",
          "cancelTimestamp"
        ]
      }
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
    },
    "required": [
      "abandonedCall"
    ]
  }
```

E.11.3 Element State Notify Body

E.11.3.1 JSON Schema

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "version": "1.0",
  "title": "Element State NOTIFY",
  "description": "SIP NOTIFY message body for Element State
notifications",
  "type": "object",
  "properties": {
    "elementState": {
      "type": "object",
      "properties": {
        "elementDomain": {
          "type": "string"
        },
        "state": {
          "type": "string"
        },
        "reason": {
          "type": "string"
        }
      },
      "required": [
        "elementDomain",
        "state",
        "reason"
      ]
    }
  },
  "required": [
    "elementState"
  ]
}
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

E.11.3.2 Queue State Notify Body

E.11.3.3 JSON Schema

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "version": "1.0",
  "title": "Queue State NOTIFY",
  "description": "SIP NOTIFY message body for Queue State notifications",
  "type": "object",
  "properties": {
    "queueState": {
      "type": "object",
      "properties": {
        "queueUri": {
          "type": "string"
        },
        "queueLength": {
          "type": "number"
        },
        "queueMaxLength": {
          "type": "integer"
        },
        "state": {
          "type": "string"
        }
      },
      "required": [
        "queueUri",
        "queueLength",
        "queueMaxLength",
        "state"
      ]
    }
  },
  "required": [
    "queueState"
  ]
{
```

E.11.3.4 Service State Notify Body

E.11.3.5 JSON Schema

```
{
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
  "$schema": "http://json-schema.org/draft-04/schema#",
  "version": "1.0",
  "title": "Service State NOTIFY",
  "description": "SIP NOTIFY message body for Service State
notifications",
  "type": "object",
  "properties": {
    "service": {
      "type": "object",
      "properties": {
        "name": {
          "type": "string"
        },
        "domain": {
          "type": "string"
        }
      },
      "required": [
        "name",
        "domain"
      ]
    },
    "serviceState": {
      "type": "object",
      "properties": {
        "state": {
          "type": "string"
        },
        "reason": {
          "type": "string"
        }
      },
      "required": [
        "state",
        "reason"
      ]
    },
    "securityPosture": {
      "type": "object",
      "properties": {
        "posture": {
          "type": "string"
        },
        "reason": {
          "type": "string"
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
            }
          },
          "required": [
            "posture",
            "reason"
          ]
        }
      },
      "required": [
        "service",
        "serviceState"
      ]
    }
```

E.11.4 Common YAML

E.11.4.1 OpenAPI Interface Description

```
components:
  schemas:
    VersionsArray:
      type: object
      required:
        - versions
      properties:
        versions:
          type: array
          items:
            type: object
            required:
              - major
              - minor
            properties:
              major:
                type: integer
                format: int32
                description: Version major number
              minor:
                type: integer
                format: int32
                description: Version minor number
              vendor:
                type: string
                description: Vendor extension of the version
              serviceInfo:
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

```
                type: object
                properties:
                  requiredAlgorithms:
                    type: array
                    items:
                      type: string
                      enum: [EdDSA, none]
                    description: alg Header Parameter Values for JWS
        fingerprint:
          type: string
          description: Vendor info
    ConditionType:
      type: string
      enum: [TimePeriodCondition, SipHeaderCondition,
AdditionalDataCondition, MimeBodyCondition, LocationCondition,
CallSuspicionCondition, SecurityPostureCondition,
            QueueStateCondition, LostServiceUrnCondition,
ServiceStateCondition, CallSourceCondition, BodyPartCondition,
RequestUriCondition,
            NormalNextHopCondition, IncomingQueueCondition,
SdpOfferCondition, CapCondition, CallingNumberVerificationStatusCondition]
    Jws:
      type: object
      required:
        - payload
        - protected
        - signature
      properties:
        payload:
          type: string
          format: byte
        protected:
          type: string
          format: byte
        signature:
          type: string
          format: byte
```


© Copyright 2011-2022 National Emergency Number Association, Inc.

Acknowledgements

The National Emergency Number Association (NENA) 9-1-1 Core Services Committee, i3 Architecture Working Group developed this document.

NENA Board of Directors Approval Date: 07/12/2021

NENA recognizes the following industry experts and their employers for their contributions to the development of this document.

Members	Employer
Steve O'Conor, ENP, 911 Core Services Committee Co-Chair, Working Group Co-Chair	Next Generation 9-1-1 Consulting Services, LLC
Terry Reese, 911 Core Services Committee Co-Chair	Ericsson
Brian Rosen, Working Group Co-Chair	Brian Rosen Technologies LLC
Dan Banks	Digital Data Technologies, Inc.
Marc Berryman, ENP	Mission Critical Partners
Daniel Biage	Solacom Technologies, Inc.
Guy Caron	Bell Canada
Jerry Eisner, ENP	RedSky Technologies
Simon Farrow	Stancil Corporation
Randall Gellens	Core Technology Consulting
Daniel Hagan	Hagan Consulting, Inc.
Jason Horning, ENP	North Dakota Association of Counties
Rafal Kaminski	Motorola Solutions, Inc.
James Kinney	INdigital Telecom
Roger Marshall	Comtech Telecommunications Corp.
Dan Mongrain	Motorola Solutions, Inc.
Darrin Morkunas	Intrado, Inc.
Philip Reichl	INdigital Telecom
Matthew Serra, ENP	Rave Mobile Safety
Brooks Shannon	RapidDeploy
Jim Shepard, ENP	911 Datamaster
Bob Sherry, ENP	West Safety Services
Michael Smith	Equature/DSS Corp.
Henry Unger	Pulsiam
Jeffrey Wheeler	Data Technical Services

© Copyright 2011-2022 National Emergency Number Association, Inc.

Special Acknowledgements:

Delaine Arnold, ENP, Committee Resource Manager, has facilitated the production of this document through the prescribed approval process.

The i3 Architecture Working Group is part of the NENA Development Group that is led by:

- Jim Shepard, ENP, and Wendi Rooney, ENP, Development Steering Council Co-Chairs
- Roger Hixson, ENP, 9-1-1 Services Senior Consultant
- Brandon Abley, Technical Issues Director
- April Heinze, Operational Issues Director

© Copyright 2011-2022 National Emergency Number Association, Inc.