# NENA Detailed Functional and Interface Standards for the NENA i3 Solution


NENA Detailed Functional and Interface Standards for the NENA i3 Solution

NENA-STA-010.2-2016 (originally 08-003)
DSC Approval: 08/16/2016
PRC Approval: 08/29/2016
NENA Executive Board Approval: 09/10/2016
Next Scheduled Review Date: Continuous review; planned development as an ANSI Standard in the next version.

Prepared by:
National Emergency Number Association (NENA) Interconnection and Security Committee, i3 Architecture Working Group

Published by NENA
Printed in USA

***© Copyright 2016 National Emergency Number Association, Inc.***

One Nation 9-1-1 One Number

**NENA STANDARD DOCUMENT**
**NOTICE**

This Standard Document (STA) is published by the National Emergency Number Association (NENA) as an information source for the designers, manufacturers, administrators and operators of systems to be utilized for the purpose of processing emergency calls. It is not intended to provide complete design or operation specifications or parameters or to assure the quality of performance for systems that process such equipment or services.

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,
- Or to reflect 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 expressed or implied is hereby granted. 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.

This document has been prepared solely for the use of 9-1-1 System Service Providers, network interface and system vendors, participating telephone companies, 9-1-1 Authorities, etc.

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 change 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 2016 National Emergency Number Association, Inc.***

## ACKNOWLEDGEMENTS

The National Emergency Number Association (NENA) Interconnection and Security Committee, i3 Architecture Working Group developed this document.

NENA recognizes the following industry experts and their employers for their contributions in development of this document.

Executive Board Approval Date 09/10/2016

| **Members** | **Employer** |
|---|---|
| Nate Wilcox, Interconnection and Security Committee Co-Chair | Emergicom |
| Steve O'Conor, ENP, Interconnection and Security Committee Co-Chair, Working Group Co-Chair | Synergem Technologies, Inc. |
| Terry Reese, Interconnection and Security Committee, NG9-1-1 Architecture Evolution Subcommittee Chair | Ericsson |
| Brian Rosen, Working Group Co-Chair | Neustar Inc. |
| Dan Banks | Digital Data Technologies, Inc. |
| Marc Berryman, ENP | Mission Critical Partners |
| Guy Caron, ENP | Bell Canada |
| Guy Churchouse, ENP | Consultant |
| Jerry Eisner, ENP | RedSky Technologies |
| Simon Farrow | Stancil Corporation |
| Randall Gellens | Qualcomm Technologies, Inc. |
| Dave Higton | NICE Systems |
| Jason Horning, ENP | North Dakota Association of Counties |
| Roger Marshall | Comtech Telecommunications Corporation |
| Dan Mongrain | Bell Canada |
| Philip Reichl | Modular Communication Systems |
| Matthew Serra, ENP | Rave Mobile Safety |
| Brooks Shannon | GeoComm |
| Jim Shephard, ENP | 911 Datamaster |
| Bob Sherry, ENP | West Safety Services |
| Michael Smith | DSS Corp. |

**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:

- Pete Eggimann ENP and Jim Shepard ENP, Development Steering Council Co-Chairs
- Roger Hixson ENP, Technical Issues Director
- Christopher Blake Carver, ENP, PSAP Operations Director

# Table of Contents





One Nation 9-1-1 One Number

One Nation 9-1-1 One Number

One Nation 9-1-1 One Number

One Nation 9-1-1 One Number

One Nation 9-1-1 One Number

One Nation 9-1-1 One Number

One Nation 9-1-1 One Number

One Nation 9-1-1 One Number

# 1 Executive Overview

This specification builds upon prior NENA publications including i3 requirements [1] and architecture [100] 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 only the detailed functional and external 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 origination networks that are non-IP as well as legacy Public Safety Answering Points (PSAPs) that interconnect to the i3 solution architecture, as described below. 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 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 interconnections. This document describes how NG9-1-1 works after transition, including ongoing interworking requirements for IP-based and TDM-based PSAPs and origination networks[2]. It does not provide solutions for how PSAPs, origination networks, Selective Routers (SRs) and ALI systems evolve. Rather, it describes the end point where 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. The NENA NG9-1-1 Transition Planning Committee (NGTPC) has produced documents covering transition options and procedures.

This document supports IP-based and legacy TDM-based PSAPs.

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 origination networks (the Legacy Network Gateway) used by origination networks who cannot yet create call signaling matching the interfaces described in this document for the ESInet. It is not envisioned that legacy origination networks will evolve to IP interconnect in all cases, and thus the Legacy Network Gateways will be needed for the foreseeable future. The document considers all wireline, wireless, and other types of networks with IP interfaces, including IP Multimedia Subsystem (IMS) [64] networks, although the document only describes the external interfaces to the ESInet/NGCS, which a

[1] As defined in Section 2.4, the term "call" includes text messages and non-human initiated alerts
[2] "Origination networks" include service providers who send calls to ESInets/NGCS.

conforming network must support. This document describes a common interface to the ESInet/NGCS, to be used by all types of origination networks or devices. How origination networks, or devices within them, conform is not visible to the ESInet/NGCS and is out of scope. NENA has endeavored to define this interface to be sufficiently aligned with the major types of origination networks, as defined by the prevalent SDOs (such as 3GPP, 3GPP2, IETF), that they are able to conform without significant modification to their architectures. However, it is recognized that IMS design has evolved in parallel with development of this document, and that the interconnection of IMS originating networks and i3 ESInets is documented in ATIS-0700015.v003 [190].

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, will 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 installed, provisioned and operated some kind of location function for their networks. Location functions are critical for 9-1-1 calls originating on an IP network because it provides a 9-1-1 valid location to IP clients that bundle their location in the SIP signaling to the ESInet.
3. All calls entering the ESInet will normally have location (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 9-1-1Authority'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 describes 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 to a legacy PSAP as well as the transfer of an emergency call from/to an i3 PSAP to/from a legacy PSAP.
10. Federal, State and local laws, regulations and rules 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 is North American-specific and may not be applicable in other areas.

# 2 Introduction

## 2.1 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 origination 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.

## 2.2 Technical Impacts Summary

This standard supports end-to-end IP connectivity; gateways are used to accommodate legacy wireline and wireless origination 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 interconnections. This document describes how NG9-1-1 works after transition, including ongoing interworking requirements for IP-based and TDM-based PSAPs and origination networks. It does not provide solutions for how PSAPs, origination networks, SRs and ALI systems evolve. Rather, it describes the end point where 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 PSAPs. 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 origination networks (the Legacy Network Gateway) used by origination networks who cannot yet create call signaling matching the interfaces described in this document for the ESInet. It is not envisioned that legacy origination 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 [64] 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 origination networks or devices. How origination networks, or devices within them, conform is not visible to the ESInet/NGCS and is out of scope. NENA has endeavored to define this interface to be sufficiently aligned with the major types of origination networks, as defined by the prevalent SDOs (such as 3GPP, 3GPP2, IETF), that they are able to conform without significant modification to their architectures.. The results of this convergence work will be documented in a future revision of this document.

## 2.3 Security Impacts Summary

This document introduces many new security mechanisms that will impact network and PSAP operations. The most significant changes to current practice 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.

## 2.4 Document Terminology

The terms "shall", "must", "mandatory", and "required" are used throughout this document to indicate normative requirements and to differentiate from those parameters that are recommendations. Recommendations are identified by the words "should", "may", "desirable" or "preferable".

This document uses the word “call” to refer to a session established by signaling with two-way real-time media and involves a human making a request for help. We sometimes use “voice call”, “video call” or “text call” when specific media is of primary importance. The term “non-human-initiated

call" refers to a one-time notification or series of data exchanges established by signaling with at most one-way media, and typically does not involve a human at the "calling" end. Examples of non-human-originated calls include a burglar alarm, an automatically detected HAZMAT spill or a flooding sensor. The term "call" can also be used to refer to either a "Voice Call", "Video Call", "Text Call" or "Data–only call", since they are handled the same way through most of NG9-1-1. The term "Incident" is used to refer to a real world occurrence 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 4.2 and 5.10.

Prior versions of this document differentiated between Additional Data about a call, caller or location. The repository for additional call data was the Call Information Database (CIDB). In this version, there is only "Additional Data" which is provided as a series of blocks regardless of the source of the data and the "Additional Data Repository" (ADR) holds Additional Data. See Sections 5.11 and 8 for more information.

### 2.5 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 Changes |
|---|---|---|
| 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 SDO liaisons, and Request for Information (RFI)-like processes. It provides more detailed specifications for interfaces and functions, compared to the prior revision 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.<br><br>Provide more detailed specification and reflect early implementation experience. Provisioning was taken out of scope and the section was removed. |



One Nation 9-1-1 One Number

## 2.6 Recommendation for Additional Development Work

This is the first revision of this document. There are several sections where 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 revision 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 revision 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 |
| 3.1.4 | The interactions of elements and services are not well articulated in this document. A future revision will provide additional clarity on how elements and services interact, and how clients use elements and services. |
| 3.5 | Note that the specification of the MSAG Conversion Service is underspecified and will be addressed in a future revision of this document. |
| 3.11 | A future revision of this document will standardize SNMP MIBs for each FE. |
| 4.1.9 | 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 revision of this document will describe the ESInet interface. |
| 4.4.8 | Further examples of call routing will be provided in a future revision of this document. |
| 4.6 | OGC 10-069r2 is not believed to be definitive enough to enable multiple interoperable implementations. A future OGC specification or a future revision of this document is needed to describe the protocol definitively. |
| 4.6 | A standard NENA schema for WFS as used in the i3 SI layer replication protocol will be provided in a future revision of this document. |
| 4.7 | For elements (such as an ECRF) which must have a corresponding DR web service, no discovery mechanism is currently specified, and will be provided in a future revision of this document. A separate discrepancy report document exists, and must be reconciled with this document. |
| 5.2.2.5 | 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 revision of this document. |

| Section | Reference to future work |
|---|---|
| 5.2.4 | Specific policy document structures will be specified for each of the policy instances defined for the ESRP in a future revision of this document. |
| 5.2.7 | ESRP Operational Considerations to be provided in a future revision of this standard. |
| 5.6 | The IETF geopriv working group is considering the definition of a geocoding protocol/service. If such a standardization effort is undertaken, and if the resulting work is suitable, it will replace this NENA-only interface in a future revision of this document. |
| 5.7.1 | Handling of media other than voice-only callbacks is incompletely specified and will be addressed in a future revision of this document |
| 5.7.1 | A new Functional Element that handles call backs, and specifically deals with the requirements for labeling such calls for IMS-based origination networks will be defined in a future revision of this document. |
| 5.7.17 | Support for testing of Policy Routing Rules will be addressed in a future revision of this document. |
| 5.8, 5.9 | There are four mechanisms specified for call transfer, due to earlier lack of agreement within the working group. There is a desire to revisit this issue and see if some options can be eliminated. |
| 5.8.2 | The EIDD contains a snapshot of the state of the Incident, as known by the sending Agency. Obtaining updates to Incident state will be defined in a future revision of this document. |
| 5.13.1 | Need recommendations on siprec metadata to improve interoperability. |
| 5.13.3.2 | In the EventTypes described below, there is a very large amount of logging including cases where information is logged at both the sender and receiver. Future revisions of this document will describe a way to control what must be logged and whether digital signatures will be deployed and their mechanism for deployment. |
| 5.13.3.2 | A description of which elements generate which log event types will be described in a future revision of this document. |
| 5.13.3.2 | Mechanisms to support blind and supervised transfer are not defined in this document and will be standardized in a future revision of this document. Logging of such transfers is still required. |
| 5.16.3 | A future revision of this document will specify a more general way to connect the Agency Locator Search Services. |
| 5.20 | The details of the Map Database Service and its interfaces will be provided in a future revision of this document. |

| Section | Reference to future work |
|---|---|
| 6.2 | The PCA CP/CPS must be in conformance with minimum standards to be provided in a future revision of this document. |
| 6.3 | Specific definitions of the roles enumerated in this section will be defined in an informational document (NENA-INF) to be referenced in a future revision of this document. |
| 7.2.2.3 | Further study is needed to determine what should be populated as the "TTT" value for calls originating from VoIP customers. |
| 7.2.2.7 | Further specification of an interworking function between MSRP and TTY will be provided in a future revision of this document. |
| 8 | Specification for the conveyance of EIDDs between agencies, systems and applications will appear in a future revision of this document. |
| 10 | PSAP Management interface will be provided in a future revision of this document. |
| Appendix A | A future revision of this document will further clarify how conversion between legacy formats and NG9-1-1 formats is accomplished. |
| Appendix A | A future revision of this document will describe how parameters in an AQS query are handled by NG9-1-1 elements. |
| Appendix B | Additional fields to allow MSAG Conversion Service to operate correctly must be added. Definition of applicable MSAG data fields a priority for i3v3. |
| App C.1.2 | The text will need to support SDP "a=suspended", which will be covered in a future revision of this document. |

## 2.7 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 origination 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 2-5 year implementation schedule. Additional work, including that identified in Section 2.6, will be needed to achieve a level of specification necessary for full functional implementation and interoperability.

## 2.8 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 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. It also may 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.

## 2.9 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 has caused the basis on 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 [141] for more on this subject.

## 2.10 Additional Impacts (non-cost related)

This effort is a part of the over-all 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 [142]. 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 transition. This document only describes external interfaces to a PSAP. The internal PSAP subsystems and the interconnection between those subsystems must change. This is the responsibility of the joint NENA/APCO NG9-1-1 PSAP Working Group.

## 2.11 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 commleadership@nena.org

### 2.12 Acronyms/Abbreviations, Terms and Definitions

See NENA-ADM-000, NENA Master Glossary of 9-1-1 Terminology, located on the NENA web site for a complete listing of terms used in NENA documents. All acronyms used in this document are listed below, along with any new or updated terms and definitions.

| Acronym (Term) | Definition/Description | New (N) / Update (U) |
|---|---|---|
| 3GPP (3RD Generation Partner Project) | The 3rd Generation Partnership Project (3GPP) is 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. | N |
| ACK (Acknowledgement) | A message to indicate the receipt of data. | N |
| 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 | N |

| Acronym (Term) | Definition/Description | New (N) / Update (U) |
|---|---|---|
| | ringing, or when the call traverses an interworking point and the intermediate trunk is seized. | |
| Additional Data | Data that further describe the nature of how the call was placed, the person(s) associated with the device placing the call, or the location the call was placed from. | U |
| ADR (Additional Data Repository) | A data storage 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. It replaces and deprecates the concept of CIDB previously defined in 08-003 v1. | N |
| AES (Advanced Encryption Standard) | A Federal Information Processing Standard (FIPS)-approved cryptographic algorithm that is used to protect electronic data. | N |
| 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. | N |
| 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). | N |
| 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. | N |

| Acronym (Term) | Definition/Description | New (N) / Update (U) |
|---|---|---|
| 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. | N |
| 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. | N |
| ANI (Automatic Number Identification) | Telephone number associated with the access line from which a call originates. | |
| 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. Please refer to: http://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. | |
| ATIS (Alliance for Telecommunications Industry Solutions) | A U.S.-based organization that is committed to rapidly developing and promoting technical and operations standards for the communications and related information technologies industry worldwide using a pragmatic, flexible and open approach. Please refer to: http://www.atis.org<br>Ref: NENA 03-507<br>Ref: NENA 08-002<br>Ref: NENA 08-504<br>Ref: NENA 57-502 | |
| B2BUA (Back to Back User Agent) | A back to back user agent is 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.<br>A logical entity that receives a request and processes it as a user agent server (UAS). In order to determine how the request should be answered, it acts as a user agent client (UAC) and generates requests. Unlike a proxy server it maintains dialog state and must participate in all requests sent on the dialogs it established. | |

| Acronym (Term) | Definition/Description | New (N) / Update (U) |
|---|---|---|
| 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. | N |
| 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) | The Common Alerting Protocol is a general format for exchanging emergency alerts, primarily designed as an interoperability standard for use among warning systems and other emergency information systems. | N |
| CDR (Call Detail Record) | A record stored in a database recording the details of a received or transmitted call (from 08-003).<br>The data information sent to the ALI computer by a remote identifying device (PBX, Call Position Identifier, …) | |
| cid (Content Identifier (Content-ID)) | An identifier used to refer to a Multipurpose Internet Mail Extensions (MIME) block. | N |
| CIDB (Call Information Database (obsolete, replaced with Additional Data Repository)) | Obsolete, see Additional Data Repository | U |
| Codec (COder/DECoder) | In communications engineering, the term codec is used in reference to integrated circuits, or chips that perform data conversion. In this context, the term is an acronym for “coder/decoder.” This type of codec combines analog-to-digital conversion and digital-to-analog conversion functions in a single chip. In personal and business | |

| Acronym (Term) | Definition/Description | New (N) / Update (U) |
|---|---|---|
| | computing applications, the most common use for such a device is in a modem. | |
| 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). Ref: NENA 02-010 Ref: NENA 02-011 | U |
| CPE (Customer Premises Equipment) | Communications or terminal equipment located in the customer's facilities – Terminal equipment at a PSAP. | |
| 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). | U |
| 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. | N |
| 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. | |
| DNS (Domain Name Server (or Service or System)) | Used in the Internet today to resolve domain names. The input to a DNS is a domain name (e.g., 67elcordia.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. | |
| 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. | |
| DSL (Digital Subscriber Line) | A "last mile" solution that uses existing telephony infrastructure to deliver high speed broadband access. DSL standards are | |

| Acronym (Term) | Definition/Description | New (N) / Update (U) |
|---|---|---|
| | administered by the DSL Forum (http://dslforum.org/). | |
| 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.<br>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 where 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. | |
| EDXL (Emergency Data eXchange Language) | The Emergency Data Exchange Language (EDXL) is a broad initiative to create an integrated framework for a wide range of emergency data exchange standards to support operations, logistics, planning and finance. | N |
| 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. | U |
| ESInet (Emergency Services IP Network) | An ESInet is 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 | U |

| Acronym (Term) | Definition/Description | New (N) / Update (U) |
|---|---|---|
| | 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, Electronic Serial Number, Emergency Service Network) | 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) | Either a 10-digit North American Numbering plan or non-NANPA 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. In the past, these numbers may have been dialable or non-dialable. As of 2012 these numbers should be non-dialable, and all new ESRKs will be non-NANPA, non-dialable ten-digit numbers. | |
| 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. | |
| EVRC (Enhanced Variable Rate Codec) | A speech codec developed to offer mobile carriers more network capacity while not increasing bandwidth requirements. | N |
| EVRC-WB (Enhanced Variable Rate Wideband Codec) | A speech codec providing enhanced (wideband) voice quality. | N |
| FAC (Facility (SS7 message)) | A message sent in either direction at any phase of the call to request an action at another exchange. | N |
| FCC (Federal Communications Commission) | An independent U.S. government agency overseen by Congress, the Federal Communications Commission regulates interstate and international communications | N |

| Acronym (Term) | Definition/Description | New (N) / Update (U) |
|---|---|---|
| | 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, | N |
| FE (Functional Element) | An abstract building block that consists of a set of interfaces and operations on those interfaces to accomplish a task. Mapping between functional elements and physical implementations may be one-to-one, one-to-many or many-to-one. | N |
| FQDN (Fully Qualified Domain Name) | The complete domain name for a specific computer, or host, on the Internet. | N |
| 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. | N |
| 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. | N |
| GeoRSS (Geodetic Really Simple Syndication) | A simple mechanism used to encode GML in RSS feeds for use with the ATOM protocol. | N |
| Geoshape (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 3D versions of same. | U |
| GIS (Geographic Information System) | A system for capturing, storing, displaying, analyzing and managing data and associated | |

| Acronym (Term) | Definition/Description | New (N) / Update (U) |
|---|---|---|
| | attributes which are spatially referenced. | |
| GML (Geography Markup Language) | An XML grammar for expressing geographical features standardized by the OGC. | N |
| GRUU (Globally Routable User agent URI) | A SIP URI which identifies a specific endpoint where a user is signed on that is routable on the Internet. | N |
| H.264/MPEG-4 | An ITU-T Recommendation and Motion Picture Expert Group standard for a video codec | U |
| 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) | Hypertext Transport 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) | N |
| IAM (Initial Address Message) | First message sent to inform the partner switch that a call has to be established on the CIC contained in the message. Contains the called number, type of service (speech or data) and optional parameters. | |
| IANA (Internet Assigned Numbers Authority) | IANA is the entity that oversees global IP address allocation; DNS root zone management, and other Internet protocol assignments. | |
| ICE (Interactive Connectivity Establishment) | A mechanism for endpoints to establish RTP connectivity in the presence of NATs and other middleboxes. | N |
| 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. | N |
| IETF (Internet Engineering Task Force) | Lead standard setting authority for Internet protocols. | |
| IM (Instant Messaging) | A method of communication generally using text where more than a character at a time is sent between parties nearly instantaneously. | |

| Acronym (Term) | Definition/Description | New (N) / Update (U) |
|---|---|---|
| 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. | N |
| IMS (Internet Protocol Multimedia Subsystem) | The IP Multimedia Subsystem comprises all 3GPP/3GPP2 core network elements providing IP multimedia services that support audio, video, text, 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. | U |
| INVITE | A SIP transaction used to initiate a session (See re-INVITE). | U |
| IP (Internet Protocol) | The method by which data is sent from one computer to another on the Internet or other networks. | |
| IPsec (Internet Protocol Security) | IPsec is the next-generation network layer crypto platform. IPsec can be found on routers, firewalls, and client desktops. | |
| IPv4 (Internet Protocol version 4) | The fourth version of the Internet Protocol; uses 32-bit addresses. | U |
| IPv6 (Internet Protocol version 6) | The most recent version of the Internet Protocol; uses 128-bit addresses. | U |
| IS-ADR (Identity Searchable Additional Data Repository) | An Additional Data Repository that provides a service that can search for Additional Data based on a sip/sips or tel URI: (e.g., Additional Data about the caller). | N |
| 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. | |
| 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 | |

| Acronym (Term) | Definition/Description | New (N) / Update (U) |
|---|---|---|
| | 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 Location Information Server (LIS) is 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 an un-upgraded legacy origination network and the NGCS. | U |
| 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:<br>• Geodetic – shape, latitude(s), | U |

| Acronym (Term) | Definition/Description | New (N) / Update (U) |
|---|---|---|
| | 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;<br>• 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 NENA Next Generation 9-1-1 (NG9-1-1) United States Civic Location Data Exchange Format (CLDXF) Standard (NENA-STA-004);<br>• Or a combination thereof. | |
| LoST (Location to Service Translation) | 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) | An NG9-1-1 Functional Element which provides an interface between an ESInet and an un-upgraded PSAP. | |
| LRF (Location Retrieval Function) | The IMS associated functional entity that handles the retrieval of location information for the emergency caller including, where 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) | The LSRG 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 | N |

| Acronym (Term) | Definition/Description | New (N) / Update (U) |
|---|---|---|
| | 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. | N |
| MDN (Mobile Directory Number) | The telephone number dialed to reach a wireless telephone. | |
| 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. | N |
| MIME (Multipurpose Internet Mail Extensions) | A specification for formatting non-ASCII messages so that they can be sent over the Internet. | N |
| MPC/GMLC (Mobile Positioning Center/ Gateway Mobile Location Center) | The MPC/GMLC serves as the point of interface to the ANSI wireless network for the Emergency Services Network. The MPC/GMLC serves as the entity which retrieves forwards, stores and controls position data within the location network. It can select the PDE(s) to use in position determination and forwards the position to the requesting entity or stores it for subsequent retrieval. In the case of a PDE with autonomous determination capability, the MPC/GMLC receives and stores the position estimation for subsequent retrieval. The MPC/GMLC may restrict access to position information (e.g., require that the Mobile Station be engaged in an emergency service call or only release position information to authorized nodes.) | U |
| 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 from | |

| Acronym (Term) | Definition/Description | New (N) / Update (U) |
|---|---|---|
| | wireless calls. | |
| MSRP (Message Session Relay Protocol) | A standardized mechanism for exchanging instant messages using SIP where a server relays messages between user agents. | N |
| MTP (Message Transfer Part) | A layer of the SS7 protocol providing the routing and network interface capabilities to support call setup. | N |
| NANP (North American Numbering Plan) | An integrated telephone numbering plan serving 20 North American countries that share telephone numbers in the +1 country code. | U |
| 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 headers while they are in transit across a traffic routing device. | N |
| NAT (Network Address Translation) | A methodology of remapping one IP address into another by modifying network address information in Internet Protocol (IP) datagram packet headers while they are in transit across a traffic routing device. | U |
| NENA (National Emergency Number Association) | The National Emergency Number Association is 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. | |
| NG9-1-1 (Next Generation 9-1-1) | NG9-1-1 is an Internet Protocol (IP)-based system comprised of managed Emergency Services IP networks (ESInets), functional elements (applications), and databases that replicate traditional E9-1-1 features and functions and provides additional capabilities. NG9-1-1 is designed to provide access to emergency services from all connected communications sources, and provide multimedia data capabilities for Public Safety | |

| Acronym (Term) | Definition/Description | New (N) / Update (U) |
|---|---|---|
| | Answering Points (PSAPs) and other emergency service organizations. www.nena.org/resource/resmgr/ng9-1-1_project/whatisng911.pdf NOTE: It is recognized that there will be a multi-year transition to NG9-1-1 beginning as early as 2010. See the NENA list of FAQs related to NG9-1-1 for more details. | |
| 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 | N |
| 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. | N |
| NTP (Network Time Protocol) | A networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks. | U |
| OASIS (Organization for the Advancement of Structured Information Standards) | An organization that promulgates standards for data interchange. | U |
| OGC (Open Geospatial Consortium) | An organization that promulgates standards for the global geospatial community. | U |
| OLI (Originating Line Information) | A parameter that conveys class of service information about the originator of a call. | U |
| Originating ESRP | The first routing element inside the NGCS. It receives calls from the BCF at the edge of the ESInet. | U |

| Acronym (Term) | Definition/Description | New (N) / Update (U) |
|---|---|---|
| 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;<br>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 and (1) Physical Includes physical signaling and interfaces. | |
| P-A-I (P-Asserted-Identity) | A header in a SIP message containing a URI that the originating network asserts is the correct identity of the caller. | U |
| 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 ESInet. | |
| 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) | The Presence Information Data Format is 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 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, | U |

| Acronym (Term) | Definition/Description | New (N) / Update (U) |
|---|---|---|
| | 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. | U |
| PSAP (Public Safety Answering Point) | Public Safety Answering Point (PSAP): An entity responsible for receiving 9-1-1 calls and processing those calls according to a specific operational policy. | |
| PSP (Provisioning Service Provider) | The component in an ESInet functional element that implements the provider side of a 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. | |
| REFER/Replaces | Use of the SIP REFER method together with a Replaces header 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. | U |
| REL (Release (message)) | An ISUP message sent in either direction to release the circuit. | U |
| RequestURI | That part of a SIP message that indicates where the call is being routed towards. SIP Proxy servers commonly change the Request ID (“retargeting”) to route a call towards the intended recipient. | |
| Resource Priority | A header used on SIP calls to indicate priority that proxy servers give to specific calls. The Resource Priority header does not indicate that a call is an emergency call (see RequestURI). | U |

| Acronym (Term) | Definition/Description | New (N) / Update (U) |
|---|---|---|
| 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 method by which standard setting bodies receive input from interested parties outside of the working group. | |
| RLC (Release Complete (message)) | An ISUP message sent to acknowledge the release (REL) message indicating that the circuit is idle afterward and can be used again. | U |
| ROH (Receiver Off-Hook) | A call state in which the recipient's hand set is not in the cradle. | N |
| ROHC (Robust Header Compression) | A standardized method to compress the IP, UDP, UDP-Lite, RTP, and TCP headers of Internet packets. | U |
| RTCP (Real-time Transport Control Protocol) | RTCP is 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. | N |
| RTT (Real Time Text) | Text transmission that is character at a time, as in TTY. | |

| Acronym (Term) | Definition/Description | New (N) / Update (U) |
|---|---|---|
| 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. | U |
| 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. | N |
| SCTP (Stream Control Transport Protocol) | SCTP is defined by IETF RFC2960 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 RFC2960 and RFC3309, 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.<br>In addition to the services specified in IETF RFC2960, 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 RFC4566. | U |
| Security Posture | An event that represents a downstream entity's current security state (normal, under attack …). | |
| Service Uniform Resource Name (Service URN) | 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 | U |

| Acronym (Term) | Definition/Description | New (N) / Update (U) |
|---|---|---|
| | 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 RequestURI. | |
| 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. | U |
| SI (Spatial Interface) | A standardized interface between the GIS and the functional elements that consume GIS data, such as the ECRF/LVF. | N |
| 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. | U |
| SIP (Session Initiation Protocol) | An IETF defined protocol (RFC3261) that defines a method for establishing multimedia sessions over the Internet. Used as the call signaling protocol in VoIP, i2 and i3 | |
| SLA (Service Level Agreement) | A contract between a service provider and the end user, which stipulates and commits the service provider to a required level of service. | |
| 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. | U |
| SOAP (Simple Object Access Protocol) | SOAP is 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 | |

| Acronym (Term) | Definition/Description | New (N) / Update (U) |
|---|---|---|
| | can build on. | |
| 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. | U |
| SR (Selective Router [a.k.a., E9-1-1 Tandem, or Enhanced 9-1-1 (E9-1-1) 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 geo 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. | U |
| SRV (Service [a DNS record type]) | A specification of data in the Domain Name System defining the location, i.e. the hostname and port number, of servers for specified services. | U |
| SS7 (Signaling System 7) | An out-of-band signaling system used to | |

| Acronym (Term) | Definition/Description | New (N) / Update (U) |
|---|---|---|
| | 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. | |
| TCP<br>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 integration model. | |
| TDM<br>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. | |
| Terminating ESRP | The last ESRP for a call in NGCS. | U |
| TLS<br>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. | U |
| TN (Telephone Number) | A sequence of digits assigned to a device to facilitate communications via the public switched telephone network or other private network. | U |
| 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. | |
| TTY (Teletypewriter [a.k.a. TDD, Telecommunications Device for the Deaf and Hard-of-Hearing]) | In 9-1-1, a device that uses a keyboard and display, and communicating with tone signaled Baudot or ASCII. | |
| TURN<br>(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. | N |
| 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. Ref: NENA 02-010 Ref: NENA 02-011 | N |
| UA (User Agent) | As defined for SIP in IETF RFC 3261[5], the | |

| Acronym (Term) | Definition/Description | New (N) / Update (U) |
|---|---|---|
| | 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.<br>"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.<br>"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<br>Universal Description, Discovery and Integration | An XML-based registry for businesses worldwide, which enables businesses to list themselves and their services on the Internet. | N |
| 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 compared to other protocols like TCP. Because UDP is widely used, and also since it has no guaranteed delivery mechanism built in, it is | |

| Acronym (Term) | Definition/Description | New (N) / Update (U) |
|---|---|---|
| | also referred to as Universal Datagram Protocol, and as Unreliable Datagram Protocol. | |
| URI (Uniform Resource Identifier) | A predictable formatting of text used to identify a resource on a network (usually the Internet)<br>OR<br>A string of characters that must follow prescribed syntaxes such as URL, URN… Note Version 1.1 of the XML namespaces recommendation uses IRIs (Internationalized Resource Identifiers) instead of URIs. However, because version 1.1 is not yet a full recommendation [February, 2003] and because the IRI RFC is not yet complete, this document continues to refer to URIs instead of IRIs. | |
| URL (Uniform Resource Locator [location sensitive]) | A URL is a URI specifically used for describing and navigating to a resource (e.g. http://www.nena.org) | |
| URN (Uniform Resource Name [location insensitive]) | Uniform Resource Identifiers (URIs) that use the URN scheme, and are intended to serve as persistent, location-independent resource names. | |
| NCCIC (National Cybersecurity and Communications Integration Center) | Part of the Department of Homeland Security's (DHS) National Cybersecurity and Communications Integration Center (NCCIC) (formerly referred to as US-CERT) serves as a central location where a diverse set of partners involved in cybersecurity and communications protection coordinate and synchronize their efforts. NCCIC's partners include other government agencies, the private sector, and international entities. Working closely with its partners, NCCIC analyzes cybersecurity and communications information, shares timely and actionable information, and coordinates response, mitigation and recovery efforts.<br>Ref: https://www.us-cert.gov/nccic | N |
| USPS (United States Postal Service) | An independent agency of the United States government responsible for providing mail service in the United States. | N |

| Acronym (Term) | Definition/Description | New (N) / Update (U) |
|---|---|---|
| UTC<br>Universal Coordinated Time | The primary time standard in the world based on the time zone in Greenwich. | U |
| VEDS (Vehicle Emergency Data Sets) | A uniform data set for the collection and transmission of Advanced Automatic Collision Notification (AACN) data by automotive Telematics Service Providers (TSPs). | U |
| 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. | U |
| 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. | U |
| 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. | U |
| WFS (Web Feature Service) | A web service that allows a client to retrieve and update geospatial data encoded in Geography Markup Language (GML). | U |
| WSDL (Web Service Definition Language) | An XML-based interface definition language that is used for describing the functionality offered by a web service. | U |
| X.509 | An ITU-T standard for a public key infrastructure (PKI) and Privilege | N |

| Acronym (Term) | Definition/Description | New (N) / Update (U) |
|---|---|---|
| | Management Infrastructure (PMI). In NG9-1-1, refers to the format of a certificate containing a public key. | |
| 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. | N |

# 3 General Concepts

## 3.1 Identifiers

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

### 3.1.1 Agency Identifier

An agency is represented by a domain name as defined in RFC 1034 [105]. Agencies must use one domain name consistently in order to correlate actions across a wide range of calls and incidents. Any domain name in the public Domain Name System (DNS) is acceptable so long as each distinct agency uses a different domain name. This implies that each agency ID is globally unique. An example of an agency identifier is “police.allegheny.pa.us”.

### 3.1.2 Agent Identifier

An agent is represented by an agent identifier that is a username, using the syntax for “Dot-string” in RFC 5321 [170] (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”.

### 3.1.3 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 3.11). The external interfaces of the element must adhere to the standards in this document. Elements are addressable via a hostname 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.

### 3.1.4 Service Identifier

A name used to represent a collection of functional elements that define a service. Services defined in this document include:

- Emergency Call Routing Function
- Location Validation Function
- Emergency Service Routing Proxy
- PSAP
- Logging Service
- MSAG Conversion Service
- Geocode Conversion Service
- Map Database Service
- Conference Bridge
- Agency Locator
- Interactive Media Response  Service
- Additional Data Repository (if hosted on an ESInet)
- Identity-Searchable Additional Data Repository (if hosted on an ESInet)
- Policy Store

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, the external interfaces of the service must adhere to the standards in this document. Services are identified with a Fully Qualified Domain Name (FQDN). An example of a Service Identifier is “psap.allegheny.pa.us”.

The interactions of elements and services are not well articulated in this document. A future revision will provide additional clarity on how elements and services interact, and how clients use elements and services.

### 3.1.5 Call Identifier

The term “call” is defined in Section 2.4 and includes voice calls, video calls, text calls and non-human-initiated calls. The first element in the first ESInet that handles a call assigns the Call Identifier. The form of a Call Identifier is a Uniform Resource Name (URN) [149] formed by the prefix “urn:nena: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:nena:uid:callid:a56e556d871:bcf.state.pa.us” would be 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 between 10 and 30 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 "nena-CallId".

### 3.1.6 Incident Tracking Identifier

A real world occurrence 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:nena: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:nena:uid:incidentid:a56e556d871:bcf.state.pa.us" would be a properly formatted Incident Tracking Identifier. The unique string must be unique for each Incident the element handles over time. One way to create this unique string is to use a timestamp with a suffix that differentiates multiple Incidents if 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 policeman 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 that handles an emergency call or declares an incident. Incident Tracking Identifiers may be assigned to a call prior to determining what real world incident it actually belongs to. (See Section 5.2.2.2). The Incident Identifier is added to a SIP message using a Call-Info header field with a purpose of "nena-IncidentId".

## 3.2 Time

It is essential that all elements on the ESInet have the same notion of time. To do so, every element must implement NTP, and access to a hardware clock must be provided in each ESInet such that the absolute time difference between any element on any ESInet and another element in the same or any other ESInet is maintained within one tenth of a second[3] of one another. (See Section 5.18).

## 3.3 Timestamp

Any record that must be marked with when it occurred (especially a log record, see Section 5.13) includes a Timestamp. A Timestamp includes integer-valued year, month, day, hour, and minute values, a decimal seconds value, and a timezone offset value. Time must include seconds, and, if two

[3] Some implementations may require more time accuracy than this specification within a domain such as an ESInet

or more Timestamps could be generated by the same element within one second where the order of events matter, the seconds element must include sufficient decimal places in the seconds field to differentiate the Timestamps. Except where otherwise dictated by standards, all time within the ESInet is represented as local time with offset from UTC. The offset is a required component of the Timestamp and consists of an integer number of hours and minutes.

Timestamps contained in XML documents governed by this specification shall be represented by the "dateTime" datatype described in *XML Schema Part 2: Datatypes Second Edition* [114], 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".

## 3.4 Events common to multiple functional elements

Events are described in Section 4.1.3.2. The following events may be implemented in any functional element. Also see the Logging service interface in Section 5.13, which is implemented by any element that handles a call.

### 3.4.1 Security Posture

SecurityPosture is an event that represents a downstream entity's current security state. This document creates a NENA Registry System (NRS) registry of allowed values. The initial defined values are:

- Green – The entity is operating normally
- Yellow – The entity is receiving suspicious activity, but is able to operate normally
- Orange – The entity is receiving fraudulent calls/events, is stressed, but is able to continue most operations
- Red – The entity is under active attack and is overwhelmed

**Event Package Name**: nena-SecurityPosture

**Event Package Parameters**: None

**SUBSCRIBE Bodies**: Standard RFC 4661 [127] + extensions filter specification may be present

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

**NOTIFY Bodies**: MIME type application/vnd.nena.SecurityPosture+xml

| Parameter | Condition | Description |
|---|---|---|
| Posture | Mandatory | Enumeration of current security posture from NRS SecurityPosture registry |

**Notifier Processing of SUBSCRIBE Requests**

The notifier consults the policy (securityPosture) to determine if the requester is permitted to subscribe. It returns 603 (Decline) if not acceptable. If the request is acceptable, it returns 202 (Accepted).

**Notifier Generation of NOTIFY Requests**

When the security posture of the element changes, a new NOTIFY request is generated, adhering to the filter requests.

**Subscriber Processing of NOTIFY Requests**

No specific action required.

**Handling of Forked Requests**

Forking is not expected to be used with this package.

**Rate of Notification**

Posture state normally does not change rapidly. Changes may occur in minutes if attacks start and stop sporadically.

**State Agents**

No special handling is required.

### 3.4.2 Element State

ElementState is an event that indicates the state of an element either automatically determined, or as determined by management. This document creates an NRS registry (ElementState) of allowed values (see Section 11.8) with initial defined states of:

- Normal: The element is operating normally
- ScheduledMaintenance: The element is undergoing maintenance activities and is not processing requests
- ServiceDisruption: The element has significant problems and is unable to process all requests
- Overloaded: The element is completely overloaded
- GoingDown: The element is being taken out of service
- Down: The element is unavailable

In addition, if the subscriber to an element is unable to contact that element, it may show the state of the element as “Unreachable”.

Note that when an implementation provides redundant physical implementations to increase reliability, usually the set of physical boxes is treated as a single element with respect to the rest of the ESInet and there is only one element state.

**Event Package Name**: nena-ElementState

**Event Package Parameters**: None

**SUBSCRIBE Bodies**: Standard RFC 4661 [127] + extensions filter specification may be present

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

**NOTIFY Bodies**: MIME type application/vnd.nena.ElementState+xml

| Parameter | Condition | Description |
|---|---|---|
| State | Mandatory | Enumeration of current state from NRS ElementState registry |
| Reason | Optional | Text containing the reason state was changed, if available |

**Notifier Processing of SUBSCRIBE Requests**

The notifier consults the policy (elementState) to determine if the requester is permitted to subscribe. It returns 603 (Decline) if not acceptable. If the request is acceptable, it returns 202 (Accepted). Notifiers must implement event rate filters, as described in RFC 6446 [112].

**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 is not expected to be used with this package.

**Rate of Notification**

State normally does not change rapidly. Changes may occur in tens of seconds if the network or systems are unstable.

**State Agents**

No special handling is required.

### 3.4.3 Service State

ServiceState is an event that indicates the state of service either automatically determined, or as determined by management. This document creates an NRS registry (ServiceState) of allowed values (See Section 11.9) with initial defined states of:

- Normal: The service is operating normally.
- Unmanned: (applies to PSAPs only) The PSAP has indicated that it is not currently answering calls.

- ScheduledMaintenance (down): The service is undergoing maintenance activities and is not accepting service requests.
- ScheduledMaintenance (available): The service is undergoing maintenance activities, but will respond to service requests, possibly with reduced availability.
- MajorIncidentInProgress: The element is operating normally, but is handling a major incident and may be unable to accept some requests.
- PartialService: Processing some requests, but response may be delayed.
- Overloaded: The service is completely overloaded.
- GoingDown: The service is being taken out of service.
- Down: The service is unavailable.

In addition, if the subscriber to a service is unable to contact that service, it may show the state of the service as "Unreachable".
Note that one or more elements may implement a service. Each element would have its own element state; the service would have an independent state.

**Event Package Name**: nena-ServiceState

**Event Package Parameters**: None

**SUBSCRIBE Bodies**: Standard RFC 4661 [127] + extensions filter specification may be present

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

**NOTIFY Bodies**: MIME type application/vnd.nena.ServiceState+xml

| Parameter | Condition | Description |
|---|---|---|
| Service | Mandatory | Name of Service |
| State | Mandatory | Enumeration of current state from NRS ServiceState registry |
| Reason | Optional | Text containing the reason state was changed, if available |

**Notifier Processing of SUBSCRIBE Requests**

The notifier consults the policy (serviceState) to determine if the requester is permitted to subscribe. It returns 603 (Decline) if not acceptable. If the request is acceptable, it returns 202 (Accepted). Notifiers must implement event rate filters, RFC 6446 [112].

**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 is not expected to be used with this package.

**Rate of Notification**

State normally does not change rapidly. Changes may occur in tens of seconds if the network or systems are unstable.

**State Agents**

No special handling is required.

## 3.5 Location Representation

Location in NG9-1-1 is represented by content in a PIDF-LO[4] document (RFC 4119 [6], updated by RFC 5139 [76] and RFC 5491 [75]) with field use for the United States as documented in the NENA Civic Location Data eXchange Format (CLDXF) [108]. An equivalent definition for Canadian addresses will be referenced in a future revision 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 5.4.1) for translating PIDF-LO to a NENA standard MSAG representation for backwards compatibility. All geodetic data in i3 uses WGS84 as the datum.

Note that the specification of the MSAG Conversion Service is underspecified and will be addressed in a future revision of this document.

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 for such calls. There are circumstances where 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. When handling non-emergency calls, it is desirable that retransmission-allowed be honored.

## 3.6 xCards

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, the identity and contact information is part of the data structure. When contact data is needed, i3 specifies the use of a vCard as defined in RFC 6350 [123] in eXtensible Markup Language (XML) format per RFC 6351 [150]. A vCard in XML form is known as an xCard.

[4] In the IETF, location information is a subset of Presence information. 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.

## 3.7 Emergency Services IP Networks

ESInets are private, managed, and routed IP networks. An ESInet serves a set of PSAPs, a region, a state, or a set of states. 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 may have a backbone ESInet either directly connecting to all PSAPs in the state, or interconnected to all county or regional ESInets. Neighboring states or regions may interconnect their ESInets. It is desirable to have a backbone national ESInet to optimize routing of traffic between distant state 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 must be used including the use of brackets when specifying a port number. Note that origination 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. Origination networks should be connected to any ESInet they regularly deliver volume traffic to via a private connection, through the BCF of that ESInet. Connection through the Internet is acceptable, preferably through a Virtual Private Network (VPN).

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 2475 [171]). Routers must respect code points: functional elements must mark packets they create with appropriate code points. The BCF must police code points for packets entering the ESInet. The following code points (from Pool 1) 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:

| DSCP | Use | PHB |
|---|---|---|
| 1 | Routine Traffic | Default |
| 5 | 9-1-1 Signaling | AF12 |
| 9 | 9-1-1 Text Media | AF12 |
| 13 | 9-1-1 Audio Media | EF |
| 17 | 9-1-1 Video Media | AF11 |
| 21 | 9-1-1 Non-human-initiated Call | AF21 |
| 25 | Intra ESInet Events | AF21 |
| 29 | Intra ESInet Other 9-1-1 Traffic | AF22 |

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 never be used with IPv6 addresses. Dynamic Host Configuration Protocol (DHCP) [184] must be implemented on all network elements to obtain IP address, gateway, and other services.

There must be no 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 disaster, deliberate attack and massive failure.

## 3.8 Service Interfaces

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

- Web services typically using a Simple Object Access Protocol (SOAP) [185] interface
- Simple HTTPS [192] GET (and in some cases, POST) with retrieval of xml data structures based on a Uniform Resource Identifier (URI)
- SIP interfaces, including SIP Subscribe/Notify

The term “web service”, when it appears in this document, unless otherwise specified, means a SOAP interface defined by a NENA provided Web Service Definition Language (WSDL).

## 3.9 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 the server (or peer) assumes with respect to redundancy.

The i3 architecture provides support for one model where 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 that could not be completed.

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

### 3.10 Telephone Numbers

Where telephone numbers are used within an ESInet, full E.164 [157] 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 [189] or in a SIP URI using the user=phone parameter.

### 3.11 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 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.

All physical realizations must provide Simple Network Management Protocol (SNMP) version 3 [91] management interfaces to network management systems.

Note: a future revision of this document will standardize Management Information Bases (MIBs) for each Functional Element (FE).

## 4 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.

### 4.1 SIP Call

The i3 call interface is SIP [12]. All calls presented to the NGCS must be SIP signaled. Calls are potentially multimedia, and can include one or more forms of media (audio, video and/or text[5]). See Section 4.1.10 for a discussion of "non-human-initiated calls" (also called "data-only emergency calls") which can be used for non-human-initiated requests for help where there is no human caller. SIP may 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

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

"Hitchhiker's Guide to SIP" [11]. 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.

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

A complete emergency call example is presented in Appendix D. Further examples will be provided in future revisions of this document.

### 4.1.1 Minimal Methods needed to handle a call

The only method absolutely required to handle a 9-1-1 call is the INVITE. The REFER method (defined in [23]) must also be supported in order to conference and transfer calls. Call takers (and thus bridges that they 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. So 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 5.1).

#### 4.1.1.1 INVITE (initial call)

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

An emergency call has a Route header obtained from the ECRF based on the location of the call, and a Request URI containing a Service URN. Nominally, the Service URN should be "urn:service:sos". In most jurisdictions, "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) would route to the primary PSAP. The first element of the NGCS encountering a call with a subservice must rewrite the Request URI to “urn:service:sos”.

The external (i.e., outside the ESInet) ECRF returns a “PSAP URI” which would be the Route header when the call enters the ESInet. 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 would query the internal ECRF (within the ESInet) with the service URN found in the PRF origination policy for the incoming call, for example “urn:nena:service:sos.psap”, and would receive 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 would still route to the same state-level ESRP, which would perform 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.

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

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 180 Ringing 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. UACs within the ESInet must generate an appropriate audible and in most cases a visual ring indication.

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. NG9-1-1 elements that initiate calls within the ESInet should appropriately respond as defined in RFC 3261 [12]. A 9-1-1 call may be so malformed that the BCF cannot parse the message.

Errors typically encountered in a SIP call should be handled as follows:

| **SIP INVITE Response Codes from ESRP** | **Description** |
|---|---|
| 180<br>(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 | Normal response to an answered call. |

| SIP INVITE Response Codes from ESRP | Description |
|---|---|
| (OK) | |
| 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 [12]. |
| 400<br>(Bad Request) | A 9-1-1 call is so malformed that the BCF cannot parse the message. |
| 401<br>(Unauthorized) | Should never occur for a 9-1-1 call, but proxy authorization is required for all calls originated by entities within an ESInet. |
| 402<br>(Payment Required) | Should never occur for a 9-1-1 call or an internal call. |
| 403<br>(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<br>(Not Found) | 404 (Not Found) would normally not occur for a 9-1-1 call, but may be used within the ESInet. |
| 406<br>(Not Acceptable) | The 406 (Not Acceptable) should not occur for a 9-1-1 call because the INVITE should not have an Accept header that is unacceptable to the PSAP. If it does, 406 is the correct response. |
| 408<br>(Request Timeout) | May be issued in an unplanned circumstance. Normally, this should never happen to a 9-1-1 call. |
| 413<br>(Request Entity too Large) | The BCF should accept any Request URI, but downstream elements may return 413 (Request Entity Too Large). |
| 414<br>(Request-URI Too Long) | The BCF should accept any Request URI, but downstream elements may return 414 (Request-URI Too Long). |
| 416<br>(Unsupported URI Scheme) | The BCF should accept any Request URI, but downstream elements may return 416 (Unsupported URI Scheme). |
| 486<br>(Busy Here) | PSAPs may limit the number of test calls, and if that limit is exceeded, the response shall be 486 Busy Here. |
| 500<br>(SIP Server Internal Error) | Indicates a failure in a system, or a failure to be able to progress the call. Depending on the source of the failure, retry may succeed. If encountered inside the ESInet, an alternate (or default) route should be tried if retry fails or is not attempted. |
| 600<br>(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. |

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, 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.

#### 4.1.1.2 REFER (transfer)

The REFER method is used within the ESInet for two purposes:

- To transfer a call
- To conference additional parties to a call

Actually, these two use cases are related, because the ESInet transfer operation involves a bridge so that the caller is never put on hold.

REFER is defined in [23]. 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 of the request. The recipient of the REFER request sends an INVITE to the URI in the Refer-To header.

REFER creates an implicit subscription [17] to a REFER event package. As with all SIP subscriptions the recipient of the REFER sends an immediate 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, 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 an REFER with Replaces request where the Replaces SIP Call ID does not exist, it must be rejected.

If the calling device supports REFER, the REFER can be sent to the calling device to transfer a call. Section 5.9 discusses the problem of a calling device that is unable to support a REFER transaction.

#### 4.1.1.3 BYE (call termination)

The BYE method is used to terminate a call. BYE may be initiated from either end. PSAPs must accept a BYE request and honor it.

Appendix C defines a mechanism for implementing PSAP control of disconnect.

### 4.1.2 Methods allowed to be initiated by any UA which must be supported by i3 elements

#### 4.1.2.1 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 [12]. CANCEL would be the signaling used to abandon a call, and NGCS elements must treat a CANCELled call as such, including logging requirements.

#### 4.1.2.2 UPDATE (update parameters)

UPDATE is defined in RFC 3311 [18] and is sometimes used during call establishment if needed to change the parameters of the call. UPDATE is usually not used on calls that are already established, which typically requires a re-INVITE. UPDATE may be used on any call within an ESInet (including 9-1-1 calls).

#### 4.1.2.3 OPTIONS (option negotiation)

OPTIONS may be used by an external caller, or inside the ESInet to determine the capabilities of the destination User Agent (UA). All endpoints within the ESInet must be capable of responding to an OPTIONS request, as defined in RFC 3261 [12].

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 need 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. An OPTIONS request from outside the ESInet is not a recommended way to determine if an emergency call would reach the PSAP. Instead, sparing use of the Test Call [59] mechanism is recommended. If OPTIONS is received from an entity outside the ESInet, it should receive a valid response from some entity inside the ESInet. 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, could respond.

#### 4.1.2.4 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 will use ACK.

#### 4.1.2.5 PRACK (reliable message acknowledgement)

The PRACK method is 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, see the example in RFC 3311 [21] where PRACK is sent by the UAS to reliably send an SDP "offer" to a UAC in an 18X response.

#### 4.1.2.6 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-human initiated 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; under normal usage each Instant Message stands alone, much like pager messages. MESSAGE requests may also be sent in the context of a dialog initiated by some other SIP request, for example in a multi-media call. For more information on MESSAGE please refer to RFC 3428 [21]. MESSAGE is part of the SIP/SIMPLE presence and messaging system.

#### 4.1.2.7 INFO

The INFO method [186] 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 [159] to request Intra-frame refresh (see Section 4.1.8.2).

### 4.1.3 Methods used within the ESInet

#### 4.1.3.1 REGISTER

Use of REGISTER is not defined in this document, but REGISTER may be used in some PSAPs for UA registration.

#### 4.1.3.2 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. SUBSCRIBE requests should contain an "Expires" header. This “Expires” value indicates the duration of the subscription. In order to keep subscriptions effective beyond the duration communicated in the "Expires" header, subscribers need to refresh subscriptions on a periodic basis using a new SUBSCRIBE message on the same dialog. The subscription also expires in the origination network when the associated SIP dialogue is terminated with a BYE.

NOTIFY messages are sent to inform subscribers of changes in state 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 several NOTIFY requests.
For further information refer to RFC 3265 [17] section 7.1.

#### 4.1.3.3 PUBLISH (update of presence information to presence server)

PUBLISH is a SIP method for publishing event state. The PUBLISH method allows the user to create, modify and remove a state in another entity which manages this state on behalf of the user. The request URI of a PUBLISH request is populated with the address of the resource for which the user wishes to publish the event state. The body of a PUBLISH request carries the PUBLISH event state. For more information refer to RFC 3911 [41].

### 4.1.4 Headers assumed supported at the interface to the NGCS

All SIP elements within an ESInet should support Robust Header Compression (ROHC) [144]. The BCF must support ROHC.

Note: The Best Current Practice for Communications Services in Support of Emergency Calling RFC 6881 [59] document referenced in this section contains normative text related to devices, originating network and service providers. This document considers only the interface between an origination network and the NGCS. References to RFC 6881 in this document are limited to requirement ED-63, the details of signaling for an emergency call. Accordingly, it shall be explicitly understood that all requirements referenced from IETF RFC 6881, regardless of wording and context in that document, shall apply only to the NGCS interface and shall in no way 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.

| Header | Defined In | See Section (or RFC 6881) | Notes |
|---|---|---|---|
| To | RFC 3261 Section 8.1.1.2 & 20.39 | ED63 2. | Usually sip:911 or "urn:service:sos" |
| From | RFC 3261 Section 8.1.1.3 & 20.20 | ED63 3. | Content cannot be trusted unless protected by an Identity header |
| Via | RFC 3261 Section 8.1.1.7 & 20.42 | ED63 4. | 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 | | NOT the NG9-1-1 call id |
| Call-Info | RFC 3261 Section 8.1.1.10 & 20.9 | | May contain Additional Data, Call and Incident Tracking IDs |
| Contact | RFC 3261 Section 8.1.1.8 & 20.10 | ED63 6. | Usually a "globally routable user agent URI" (gruu)[187] |
| Content-Length | RFC 3261 Section 20.14 | | |
| Content-Type | RFC 3261 Section 8.2.3 & 20.15 | | Used in, for example, in RFC 4119 and RFC 4566[6] |
| Geolocation | RFC 6442 | ED63 9. | |
| Geolocation-Routing | RFC 6442 | ED63 9. | Specifies if Geolocation header field can be used for |

[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.

| Header | Defined In | See Section (or RFC 6881) | Notes |
|---|---|---|---|
| | | | routing |
| History-Info | RFC 4244 | | Indicates call has been retargeted |
| P-Access-Network-Info | RFC 3325 | | May contain cell site info in carrier specific formats |
| P-Asserted-Identity | RFC 3325 | | When present, typically overrides From |
| P-Preferred-Identity | RFC 3325 | 4.1.1.14, 7.1.2.3 | Used with unauthenticated (e.g., NSI) calls |
| Reason | RFC 3326 | | Used with History Info to specify why a call was retargeted |
| Route | RFC 3261 Section 20.34 | ED63 5. | Usually ESRP/PSAP URI |
| Supported | RFC 3261 Section 8.1.1.9 & 20.37 | ED63 8. | |
| Replaces | RFC 3891 | 5.8 | Used with transfer |

### 4.1.5 Headers Accepted and also used internally

| Header | 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 | |
| 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 | |

| Header | Defined In | Notes |
|---|---|---|
| | 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 | |
| Call-Info | RFC 3261 20.9 | Used to carry URIs to Additional Data |
| Error-Info | RFC 3261 20.18 | |
| Alert-Info | RFC 3261 20.4 | |
| In-Reply-To | RFC 3261 | |

| Header | Defined In | Notes |
|---|---|---|
| | 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 3265 7.2.1 | |
| Allow Events | RFC 3265 7.2.2 | |
| Subscription-State | RFC 3265 7.2.3 | |
| Replaces | RFC 3891 | |
| Resource Priority | RFC 4412 3.1 Section 4.1.6 | |

### 4.1.6 Resource Prioritization

The Resource-Priority header (RFC 4412 [47]) 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 must be able to set Resource-Priority. All SIP proxy servers in the ESInet must implement Resource-Priority and process calls in priority order when a queue of calls is waiting for service at the proxy server and, where needed, pre-empt lower priority calls[7]. BCFs[8] must police Resource-Priority for incoming SIP calls: those 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:

[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

| 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 |

### 4.1.7 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 (RFC 4244 [44]) and the associated Reason parameter. Elements that retarget a call must add a History-Info header indicating the original intended recipient, and the reason 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.

### 4.1.8 Media

All call handling elements must support media using Real Time Protocol (RTP) (RFC 3550 [13]). 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 [14]) 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 support all media if offered, except that a legacy PSAP on a Legacy PSAP Gateway may only support audio and Teletypewriter (TTY).

#### 4.1.8.1 Audio

All User Agents in the ESInet must support g.711 mu-law and a-law codecs. A-law support is required in those cases where devices manufactured primarily for non-North American markets are used within North America. It is recommended that AMR, AMR-WB, EVRC [137], EVRC-B [138], EVRC-WB [139], and EVRC-NW [140] codecs also be supported.

#### 4.1.8.2 Video

All User Agents in the ESInet 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 must support both RFC 5104 [158] and RFC 5168 [159] 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. In order to maintain the ability to support rapid finger-spelling for sign language users, ESInet elements must attempt to maintain 30 frames per second video if offered by the sender. RTP/AVPF (RFC 4585 [160]) must be supported and is preferred in offers.

#### 4.1.8.3 Real-Time Text

All call handling elements in the ESInet must support Framework for Real-Time Text over IP Using the Session Initiation Protocol (SIP) (RFC 5194 [116]).

#### 4.1.8.4 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 [117] Real Time Text is usually the only practical way to send TTY across an IP network. If at all practical, transcoding should occur in the origination network as close to the TTY as possible. However, it is very difficult to assure that all origination networks will do that transcoding. Therefore, ESInets must have the ability to transcode. LNGs and LSRGs must transcode, and therefore it is the VoIP origination networks that are problematic in that they may present calls containing Baudot tones to the ESInet. A transcoder must be placed as early in the media path as possible[9], and the IP network between the origination 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 [118] 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 may need to handle TTY in another way, which is outside the scope of this document.

### 4.1.9 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) [10], with location and the ability to support location updates.

Note: 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 the Extensible Messaging and Presence Protocol (XMPP). At this time, the only standardized IM protocol fully specified for supporting emergency IMs within or presented to an ESInet is MSRP.

All call handling elements within the ESInet must support the Message Session Relay Protocol (MSRP) (RFC 4975 [120]), Relay Extension for the Message Session Relay Protocol (MSRP) (RFC 4976 [121]) and Multiparty Chat using the Message Session Relay Protocol (MSRP) [160].

---

[9] 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.

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



One Nation 9-1-1 One Number

Location must be included in a Geolocation header 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.

### 4.1.10 Non-human-initiated calls

Non-human-initiated 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-human-initiated calls[11] (also called data-only emergency calls) presented to an ESInet are signaled with a SIP MESSAGE method containing a Common Alerting Protocol (CAP) [94] message, possibly wrapped in an Emergency Data eXchange Language – Distribution Element (EDXL-DE) [110] wrapper. The <area> element of the CAP message is copied, in PIDF-LO form, in a Geolocation header of the SIP MESSAGE container. The CAP message is included the body of the SIP MESSAGE, with a MIMEtype of application/common-alerting-protocol+xml.

The MESSAGE should contain a Call-Info header field with a URI of one or more Additional Data blocks.

The <identifier> in the CAP message is not the same as the Call Identifier assigned in the ESInet, but the log contains the record that relates the two.

The <sender> should be the same as the "From" header in the MESSAGE.

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

An <info> element must be included. The element must contain an <event code>. The <valueName> may be some externally defined namespace, but in many cases is expected to be "NENA". This document defines a NRS registry of allowed values for "NENA- ExternalEventCodes" which registers values that may be used in an <event code> where <valueName> is "NENA". The initially defined values in the registry (which become the <value> contents in the <event code> element) are VEDS and BISACS, representing the standard Vehicle Emergency Data Set, and the NIST Building Information And Control System messages.

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 in the MESSAGE must have the PIDF-LO equivalent of the <polygon> or <circle> element(s).

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

A digital signature should be included in the CAP message. The CAP message should not be encrypted. Transport Layer Security (TLS) must be used on the SIP MESSAGE transmission to encrypt the message, with fallback (See Section4.1.12).

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-human-initiated 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-human-initiated 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 as inputs to direct calls with specified characteristics to specific entities.

There is no mechanism specified to handle an APCO/CSAA 2.101.2-2014 [191] Alarm within the ESInet, although a PSAP could have an interface to such an alarm. Future alarm systems should use the mechanism described in this section.

### 4.1.11 Bodies in messages

All SIP elements in an ESInet must support multipart MIME as defined in RFC 2046 [122]. For example, location and SDP may be present in a message body. All SIP elements must allow additional body content (for example, images, xCards, etc.) to pass to the PSAP.

### 4.1.12 Transport

SIP signaling within the ESInet must be TCP with TLS. All SIP elements must support TLS, TCP and UDP transport. Fallback to UDP is allowed. However emergency call messages have many large elements, for example, a PIDF-LO, and are more likely to be fragmented when carried in UDP[12]. Fragmentation and reassembly must be supported by all ESInet elements. If TLS establishment fails, fallback to TCP/UDP without TLS is allowed. If fallback without TLS happens, 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. Media streams for voice, video and text must be carried on RTP over UDP. All endpoints in an ESInet must implement media security with SRTP as defined in RFC 3711 [124] and SDP Security Descriptions for Media Streams (SDES) as defined in RFC 4568 [125]. SRTP Security must be requested in all calls originated within an ESInet. If a call is presented to the ESInet with SRTP, SRTP must be maintained through the ESInet[13]. Since media are routinely

[12] 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.

[13] 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.

logged, the logger 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 [13] and SRTCP as defined in RFC 3711 [124] must be supported within the ESInet and it is highly recommended that all calls presented to the ESInet provide RTCP.

PSAPs must 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 reestablish 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. In no circumstances should a call be automatically taken down just because RTP streams fail. For example a multimedia stream which loses one of several streams should not be terminated, except by call taker action.

PSAPs should supply audible ring as (early) media for devices that do not perform local audible ring or its equivalent.

### 4.1.13 Routing

All SIP elements must support routing of SIP messages per RFC 3261 [12] and RFC 3263 [15]. 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 [106] will need to 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 SIP elements in the ESInet, can be used to perform re-home on an established SIP dialog in the case of host failure.

### 4.1.14 Originating network Interface

The originating call interface to the ESInet is a SIP call interface as described above in section 4.1. 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, civic or geo, by reference or value. The location used to query the routing function must be included in the Geolocation header of the outgoing INVITE or MESSAGE method. The call must be routed, using normal RFC 3261 [12] procedures, to the URI obtained from the routing function using the "urn:service:sos" service URN. A callback address must be included in the outgoing INVITE or MESSAGE method, with an immediate device callback in the Contact header and an address of record for later callback in either the "From" header (protected by the Identity header) 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 must include at least two Call-Info header fields containing URIs that refer to Additional Data [143] "ProviderInfo" and "ServiceInfo" structures. This is indicated by the 'purpose' parameters value starting with "purpose=EmergencyCallData.ProviderInfo" and "purpose=EmergencyCallData.ServiceInfo".

Additional Call-Info header fields may be included that contain a URI(s) that refers to other Additional Data blocks. Some providers will 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 is not marked with an emergency service URN, the call should be assumed to be an emergency call.

### 4.1.15 PSAP Interface

The PSAP call interface is a SIP call interface as described in Section 4.1. All calls will be presented to the PSAP based on the terminating ESRP's Policy Routing Function (PRF), defined in section 5.2.1.5. The Geolocation header, Call-Info header fields and other headers should be the same as above (Section 4.1.14). The call will be routed, using normal RFC 3261 [12] procedures, to the URI obtained from the ESRP's PRF. See Section 5.7.1 for other information on the PSAP interface.

### 4.1.16 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 [113]). Simple mechanisms to handle overload are insufficient. Elements must not return 486 Busy Here unless it is certain, by design and configuration that the upstream element can reliably cope with the error. 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 [79].

### 4.1.17 Maintaining connections and NAT Traversal

All elements in an ESInet that implement SIP interfaces must comply with RFC 5626 [109] (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 5245 [128]. ESInets should maintain a "Traversal Using Relays around NAT (TURN)" [156] server for use by entities inside the ESInet placing calls towards the Internet.

## 4.2 Location

Location is fundamental to the operation of the 9-1-1 system. Location is provided outside the ESInet, 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. For the purposes of this document, the only capabilities a LIS provides that are relevant to i3 are:

a) A dereference function defined below for location by reference
b) Validation of location stored in the LIS by querying the i3 LVF for civic addresses

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.

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 [10] of the SIP message. It also supports location by reference, where a location URI is populated in the Geolocation header. All elements in an ESInet that use location by reference must implement SIP and HTTP Enabled Location Delivery (HELD) [9] dereferencing 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 [31]). An element needing location that has a SIP location URI must issue a SIP SUBSCRIBE (RFC 3265 [17]) to the location URI. Filters (RFC 4661 [127], RFC 6446 [112] and RFC 6447 [102]) may be used to control notification.

An element needing location that has a HELD URI must dereference per RFC 6753 [78].

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. Elements in the ESInet 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 dereferencing (although the value should be logged). Each element must do its own dereference operation, supplying its credentials to the LIS. It is recommended that LISs cache location values and supply the cached values if multiple dereferences 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 Authority (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 dispatch 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 location information changes, a new PIDF-LO with a different <provided-by> element must be created and passed in addition to the original location. The vehicle for passing this information is an EIDD.

Other than the above, the implementation used within the origination and access networks for support of location is out of scope of i3[15].

[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] The roles of the access and origination 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.

## 4.3 Policy

Policy is stored into and retrieved from the Policy Store using a web service. Section 4.3.1 below describes the "Policy Store Web Service" that facilitates agencies uploading and retrieving policies. Policies are named by the function that defines the policy i.e., the DownstreamRoutingPolicy for an ESRP. A specific policy set is known by that name and the agency whose policy is being stored or retrieved. The authentication to the web service identifies the agency storing or retrieving policy sets in the store.

The Policy Store only accepts or delivers complete policy sets, not individual rules within a policy set. The Policy Store may reduce the size of the chunk returned if it is unable or unwilling (by local policy) to serve a chunk as large as the requester specifies. 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. The response may not return the policy requested. Instead, it may return a referral to another Policy Store that may have the policy.

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 can also allow an agency to store policies on behalf of another agency. The interface includes a chunking mechanism that can be used by either the client or the server to limit the size of an individual transaction.

### 4.3.1 Policy Store Web Service

This web service has the following functions:

RetrievePolicy: Retrieves a policy set from the common Policy Store. The function’s parameters include the policy name, the identity of the agency whose policy is needed, and an indication of the maximum size of the return. The response is the policy set if it is smaller than the indicated maximum size or, if the policy is too large to send in the response, the first chunk of the policy set plus an identifier that can be used with MoreRetrievePolicy to obtain more chunks, and an expiration time. The Policy Store may reduce the size of the chunk returned if it is unable or unwilling (by local policy) to serve a chunk as large as the requester specifies. 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. The response may not return the policy requested. Instead, it may return a referral to another Policy Store that may have the policy.

**RetrievePolicyRequest**

| Parameter | Condition | Description |
|---|---|---|
| policyName | Mandatory | The name of the policy |
| agency | Mandatory | The agency whose policy is requested. Must be a domain name or URI that contains a domain name |
| maxChunkSize | Optional | Maximum size of a chunk accepted, in bytes. If not specified, responder may choose the size. |

**RetrievePolicyResponse**

| Parameter | Condition | Description |
|---|---|---|
| policyDataChunk | Optional | All or part of a policy, limited to the maxChunkSize, or smaller |
| TTL | Optional | The expiration time of the policy |
| nextChunkId | Conditional, must be present if policyDataChunk is returned, but is not the complete policy | Id to be used with MoreRetrievePolicy. |
| Referral | Optional | URI of another Policy Store that may have this policy. |
| statusCode | Optional | Response from operation |

Status Codes

200 Okay No error (optional to return)

501 Unknown or bad Policy Name

502 Unknown or bad Agency Name

503 Not available here, no referral available

504 Unspecified Error

MoreRetrievePolicy: Retrieves another chunk of a large policy set. The request includes the identifier returned to the requester in a RetrievePolicy or prior MoreRetrievePolicy operation and an indication of the maximum size of the return. The response is the next chunk of the policy set, plus an identifier that can be used on a subsequent invocation of MoreRetrievePolicy. The Policy Store may reduce the size of the chunk returned if it is unable or unwilling (by local policy) to serve a chunk as large as the requester specifies. The Policy Store must be able to accept and respond to a request it has already sent (that is, the identifiers may be used repeatedly, in case of error). The identifiers can be expired in a reasonable time period (perhaps 30 minutes).

**MoreRetrievePolicyRequest**

| Parameter | Condition | Description |
|---|---|---|
| nextChunkId | Mandatory | ChunkId returned from RetrievePolicy |
| maxChunkSize | Optional | Maximum size of a chunk accepted, in bytes. If not specified, but maxChunkSize was specified in RetrievePolicy, use that size. If neither specified, responder may choose size. |

**MoreRetrievePolicyResponse**

| Parameter | Condition | Description |
|---|---|---|
| policyDataChunk | Mandatory | Remainder or part of a policy, limited to the maxChunkSize, or smaller |
| nextChunkId | Optional | Id to be used with MoreRetrievePolicy if not the last chunk |
| statusCode | Optional | Response from operation |

Response Codes

200 Okay No error (optional to return)

504 Unspecified Error

505 Bad chunkId

StorePolicy: Initiates the storage of a policy set in the Policy Store. This function's parameters include the name of the policy, the agency whose policy is being stored, the size of the entire policy set, the expiration time, and the maximum chunk size the sender is willing to send. If the name of the agency is omitted, the sender's identity is used. The response contains the maximum size of the initial chunk, which must be no larger than the sender's maximum chunk size, and an identifier to be used with the MoreStorePolicy function.

**StorePolicyRequest**

| Parameter | Condition | Description |
|---|---|---|
| policyName | Mandatory | The name of the policy |
| agency | Mandatory | The agency whose policy is being stored. Must be a domain name or URI that contains a domain name |
| policySize | Mandatory | Size of the entire policy in bytes |
| TTL | Mandatory | The expiration time of the policy |
| maxChunkSize | Optional | Maximum size of a chunk to be sent, in bytes. If not specified, responder may choose the size. |

**StorePolicyResponse**

| Parameter | Condition | Description |
|---|---|---|
| maxChunkSize | Optional | Maximum size of a chunk accepted, in bytes. If not specified, sender may choose the size up to the maxChunksize specified in the |

| Parameter | Condition | Description |
|---|---|---|
| | | request. |
| nextChunkId | Optional | Id to be used with MoreStorePolicy. |
| statusCode | Optional | Response Code |

Status Codes

200 Okay No error (optional to return)

501 Unknown or bad Policy Name

502 Unknown or bad Agency Name

504 Unspecified Error

509 Policy Too Large

510 Bad TTL

MoreStorePolicy: Sends a chunk of the policy set to the store. Its parameters include the identifier returned from StorePolicy or a prior invocation of MoreStorePolicy, and a chunk of the policy set. The response contains the maximum size of the next chunk (which must be no larger than the maximum chunk size indicated by the sender on the original StorePolicy invocation) and an identifier to be used on a subsequent MoreStorePolicy to send the next chunk. Identifiers may be reused, but if they are, any later chunks are discarded by the store and must be re-sent. Identifiers may be expired in a reasonable time (perhaps 30 minutes).

**MoreStorePolicyRequest**

| Parameter | Condition | Description |
|---|---|---|
| nextChunkId | Mandatory | ChunkId returned from RetrievePolicy |
| policyDataChunk | Mandatory | All or part of a policy, limited to the maxChunkSize, or smaller |

**MoreStorePolicyResponse**

| Parameter | Condition | Description |
|---|---|---|
| maxChunkSize | Optional | Maximum size of a chunk accepted, in bytes. If not specified, but maxChunkSize was specified in the StorePolicyRequest, use that size. If neither is specified, responder may choose size. |
| nextChunkId | Conditional, must be supplied if not the last | Id to be used with MoreRetrievePolicy if not the last chunk |

| Parameter | Condition | Description |
|---|---|---|
| | chunk | |
| statusCode | Optional | Response from operation |

Status Codes

200 Okay No error (optional to return)

504 Unspecified Error

505 Bad chunkId

511 Chunk Too Big

EnumeratePolicies: Returns a list of policy names available in the store for a specific agency. The parameters of the request include the name of the policy set and the name of the agency. The response includes a list of the policy names in the store, the last date they were stored, expiration time, and the size of the policy. The enumeration includes only those policies that are actually stored in this specific instance of the Policy Store.

**EnumeratePoliciesRequest**

| Parameter | Condition | Description |
|---|---|---|
| policyName | Mandatory | The name of the policy. May be "*" for all policy names |
| Agency | Mandatory | The agency of interest. Must be a domain name or URI that contains a domain name or "*" for all agencies |

**EnumeratePoliciesResponse** (may be repeated for each policy)

| Parameter | Condition | Description |
|---|---|---|
| policyName | Mandatory | The name of the policy. |
| Agency | Mandatory | The agency of interest. Must be a domain name or URI that contains a domain name |
| policySize | Mandatory | Size of the entire policy in bytes |
| TTL | Mandatory | The expiration time of the policy |
| lastModification | Mandatory | Date/Time of last modification |
| statusCode | Optional | Response from operation |

Status Codes

200 Okay No error (optional to return)

501 Unknown or bad Policy Name

502 Unknown or bad Agency Name

504 Unspecified Error

The Policy Store is replicated and distributed. There is a single authoritative master store for a given policy, and there may be one or more replicas of that policy in other Policy Stores. To create a replica, the master Policy Store is provisioned with a list of replicas that are authorized. The replica uses the RetrievePolicy function to get policies from the master Policy Store, and refreshes them automatically when they expire. EnumeratePolicies can be used to determine which agency's policies are stored in the Policy Store.

As an optimization, the replica can make use of the UpdatedPolicies function:

UpdatedPolicies: Returns a list of policies updated in the Policy Store since a given time. The request includes a Timestamp. The response is a list of policy names and agencies whose policy has been updated since the Timestamp in the request.

**UpdatedPoliciesRequest**

| Parameter | Condition | Description |
|---|---|---|
| policyName | Mandatory | The name of the policy. May be "*" for all policy names |
| agency | Mandatory | The agency of interest. Must be a domain name or URI that contains a domain name or "*" for all agencies |
| updatesSince | Mandatory | Earliest time desired in the response |

**UpdatedPoliciesResponse** (may be repeated for each policy)

| Parameter | Condition | Description |
|---|---|---|
| policyName | Mandatory | The name of the policy. |
| agency | Mandatory | The agency of interest. Must be a domain name or URI that contains a domain name |
| policySize | Mandatory | Size of the entire policy in bytes |
| TTL | Mandatory | The expiration time of the policy |
| lastModification | Mandatory | Date/Time of last modification |
| statusCode | Optional | Response from operation |

Status Codes

200 Okay No error (optional to return)

501 Unknown or bad Policy Name

502 Unknown or bad Agency Name

504 Unspecified Error

UpdatedPolicies can be used as a poll to keep a more up to date replica, rather than waiting for expiration times. Use of UpdatedPolicies is recommended for replicas of policies that may reasonably be changed unexpectedly, such as in a disaster situation.

The EnumerateAgencies 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 EnumerateAgencies function (with a list of other Policy Stores provisioned in a specific Policy Store).

### 4.3.2 Route Policy Syntax

This section summarizes the syntax and semantic of the policy language used for making call routing decisions. Policy is represented in an RFC 4745 [146]-compliant common policy schema.

A policy document is an XML document, formatted according to the schema defined in RFC 4745. This document inherits the MIME type of common policy documents, namely application/auth-policy+xml. As described in RFC 4745, this document is composed of rules that contain three parts - conditions, actions, and transformations. The conditions statement may either evaluate to 'true' or 'false'. If it evaluates to 'true' then the action, and the transformations part of the rule is executed. In order to deal with the case where multiple conditions parts evaluate to 'true', a conflict resolution mechanism is described to avoid conflicting actions to be executed. Common Policy (RFC 4745) describes a conflict resolution framework and this document extends it with a priority-based mechanism whereby each rule has an associated priority value that indicates the relative importance of the specific rule with the semantic that a higher value gets precedence over a rule with a lower value. The transformations part of a rule is not used by this application.

#### 4.3.2.1 Condition Elements

This section describes the additional enhancements of the conditions part of the rule. This document inherits the Common Policy functionality, including <validity>. The <identity> and <sphere> condition is not used by this version of the document.

##### 4.3.2.1.1 Time Period Condition

The <time-period> element allows a rule to make decisions based on the time, date and time zone. It defines an extended version of the <validity> element. The <time-period> element may contain the following attributes:

dtstart: Start of interval (Timestamp, see Section 3.2). This attribute is mandatory.

dtend: End of interval (Timestamp). This attribute is mandatory.

timestart: Start of time interval in a particular day. It is of the LOCAL TIME data type as mentioned in Section.3.3.12 of RFC 5545 [172]. This attribute is optional. The default value is 000000.

timeend: End of time interval in a particular day. It is of the LOCAL TIME data type as mentioned in Section.3.3.12 of RFC 5545 [172]. This attribute is optional, but if specified, must always be greater than the value of timestart. The default value is 235959.

byweekday: List of days of the week. This attribute is optional. The "byweekday" attribute specifies a comma-separated list of days of the week. "MO" indicates Monday, "TU" indicates Tuesday, "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.

The <time-period> is based on the description in Call Processing Language, RFC 3880 [162], but with a reduced feature set.

Here is an example of the time-period element:

```
<time dtstart="20070112T083000+05"
    timestart="0800"
    timeend="1800"
    byweekday="MO,TU,WE,TH,FR"
    dtend="20080101T183000+05"/>
```

The following aspects need to be considered:

1. By default, if all the OPTIONAL parameters are missing, <time-period> element is valid for the whole duration from 'dtstart' to 'dtend'.
2. The 'byweekday' attribute comes into effect only if the period from 'dtstart' till 'dtend' is long enough to accommodate the specified values, else it is just neglected.
3. If the values of the 'byweekday' attribute values do not correspond to the expected values, they are simply ignored.
4. Only a single 'byweekday' attribute MUST be listed in a <time> element.
5. When multiple timestart and timeend values are specified, they must be specified in equal numbers and for each timestart-timeend pair, timeend must be greater than timestart but smaller than the next timestart. Failure to do so will cause all timestart and timeend values to be ignored.

#### 4.3.2.1.2 SIPHeader Element

Any header in a SIP message, such as the “From”, “To”,” Contact”, etc. can be used to perform actions on incoming messages. The <SIPHeader> element has three child elements, namely <header>, <operator> and <content>. Two operators are defined: equality match and “Is”. The equality operator is "=" and the content is compared against the value of the header. The operator “equal” may be encountered in backwards-compatible implementations.

The “Is” operator uses a registry (See Section 11.23) for <content>. The values defined in this document for content are “missing” and “erroneous”. This operator tests the header for the condition in the content. The value “missing” means the header is not present. The value “erroneous” means the header has some error noticed by the ESRP.

#### 4.3.2.1.3 Additional Data

The <additional-data> element contains four child elements:

- <type> which is a block type beginning with "EmergencyCallData."
- <element> that contains a tag (element name) of one of the elements in the Additional Data blocks.
- <operator> which may be one of "=", "<>", ">", "<",">=", "<="
- <content> a value to be compared with the <element> value using the <operator>

A typical use for this element is to route based on the class of service components, or on language preferences.

#### 4.3.2.1.4 MIME Body List Condition

The <mime-list> element contains one or more child <mime> child elements. Any mime type listed in the <mime> element is compared with the content of the incoming message.

The <mime-list> condition element evaluates to TRUE if any of its child elements evaluate to TRUE, i.e., the results of the individual child element are combined using a logical OR.

#### 4.3.2.1.5 Location Conditions

This document re-uses the location-based condition elements from RFC 6772 [145] on the location used for routing. In addition, any element of the location can be used with the syntax PIDF<element name>.

#### 4.3.2.1.6 Call Suspicion Condition

This document allows the spam-score header of the SIP message to be evaluated. The <callsuspicion> element has one child element, <score>: which indicates the spam score in the attributes "from" and "to".

#### 4.3.2.1.7 SecurityPosture Condition

The <SecurityPosture> element expressed carries a "domain" attribute where "domain" is a hostname, or a URI. If a URI is specified, the domain function is used to extract the domain from the URI. The domain must be that of an agency or element that the ESRP can subscribe to the SecurityPosture package for.

#### 4.3.2.1.8 QueueState Condition

The <QueueState> element carries a "queue" attribute, where "queue" is the name of a queue. The value of the <QueueState> element can either be:

- Active: one or more entities are actively available or are currently handling calls being enqueued
- DiversionRequested: a queue designated for diversion (i.e., not the normal call path) is having calls enqueued on it
- Inactive: no entity is available or actively handling calls being enqueued
- Disabled: The queue is disabled by management action and no calls may be enqueued

In addition, if the ESRP is unable to reach the queue, it would show the queue state as “unreachable” to the PRF.

#### 4.3.2.1.9 LostServiceURN Condition

The <LoSTServiceURN> element carries the Service URN (either urn:service:... or urn:nena:service:...) attribute. The condition evaluates to True if the Location to Service Translation (LoST) query was successful and false if it was not. If the query succeeded, the resulting URI is a variable called "Normal-NextHop", available to the rule evaluation system for subsequent rules.

Rules may make use of the following variables. Several rules require the ESRP to use the SIP-based notification mechanism described in RFC 3265 [17] to obtain the value of the variable.

#### 4.3.2.1.10 Element State

ElementState is expressed as ElementState.domain where <domain> is a hostname, or a URI. If a URI is specified, the Domain function is used to extract the domain from the URI. The domain must be an element that the ESRP can subscribe to the ElementState package for.

#### 4.3.2.1.11 Service State

ServiceState is expressed as ServiceState.<domain> where <domain> is a hostname, or a URI. If a URI is specified, the Domain function is used to extract the domain from the URI. The domain must be that of a service (such as a PSAP) that the ESRP can subscribe to the ServiceState package for.

#### 4.3.2.1.12 Call Source

CallSource (as defined in the Via headers 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 returned. If there are no originating networks, CallSource returns the domain of the caller.

#### 4.3.2.1.13 Body

Any element in a Body that is included in the message which is XML encoded, expressed as Body <mimetype><element tag>. If a Body contains more than one part (of a multipart) with the same mimetype, only the first part with that mimetype can be used. This capability may be used to route on parameters in a CAP message.

#### 4.3.2.1.14 Request URI

The URI associated with the call. Normally this would be “urn:service:sos”, but may be different for calls to an admin line, etc.

#### 4.3.2.1.15 Normal-NextHop

The URI retrieved from the LoST query.

#### 4.3.2.1.16 Incoming Queue

The URI of queue the call was received on.

#### 4.3.2.2 Actions

As stated in RFC 4745 [146], conditions are the 'if'-part of rules, whereas actions form the 'then'-part. The actions and transformations parts of a rule determine which operations the proxy server must execute on receiving a connection request attempt that matches all conditions of this rule. Actions and transformations permit certain operations to be executed.

##### 4.3.2.2.1 Priority

Each rule has to contain an unsigned integer value to indicate its priority in the <priority> element. When the conditions of two rules evaluate to 'true' then the rule with the higher priority value wins i.e., the actions of that rule will be executed. Every rule must have a unique priority value.

##### 4.3.2.2.2 Route Action

The action supported in this section is forwarding of SIP messages to a specific URL. The <route> element contains two child elements namely <recipient> and <cause>, where <recipient> contains a URI that will become the Route header for the outgoing SIP message (the Request URI is normally a service URN), and the <cause> contains the value used with the Reason header associated with a History-Info header. The <recipient> element is mandatory, and the <cause> element is optional. The <cause> values are defined in a Registry that this document establishes (Section 11.13).

##### 4.3.2.2.3 Busy Action

The <busy> element returns 600 Busy Everywhere to the caller.

##### 4.3.2.2.4 Notify Action

The <notify> element has several child elements (<recipient>, <eventCode>, <urgency>, <severity>, and <certainty>) and sends a NOTIFY message containing a CAP message to any entity subscribing to the Normal-NextHop's ESRPnotify event for that reason code. This may be used, for example, to advise other entities that calls are being diverted, etc. If the <recipient> is a service URN, the CAP message is wrapped in a SIP MESSAGE and is routed via the ECRF to the proper recipients. All indicated child elements provide information on how to populate the CAP message.

#### 4.3.2.3 Examples

```
<?xml version="1.0" encoding="UTF-8"?>
<ruleset xmlns="urn:ietf:params:xml:ns:common-policy"
  xmlns:nena="urn:nena:xml:ns:policy.policy-v1"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

      ; Call is probably spam.
       <rule id="AA56i12">
    <conditions>
          <nena:callsuspicion>
                <nena:score from="70" to="100"/>
              </nena:callsuspicion>
    </conditions>
    <actions>
          <priority>7</priority>
      <nena:route>
```



One Nation 9-1-1 One Number

```
<nena:recipient>sip:special-treatment@psap.foo-bar.com
          </nena:recipient>
        </nena:route>
      </actions>
    </rule>

        ; Rule for handling a SIP msg contain a CAP payload.
        <rule id="AA56i11">
      <conditions>
            <nena:mime-list>

<nena:mime>application/common-alerting-protocol+xml</nena:mime>
            </nena:mime-list>
      </conditions>
      <actions>
            <priority>6</priority>
        <nena:route>
                  <nena:recipient>sip:psap@home.foo-bar.com
          </nena:recipient>
        </nena:route>
      </actions>
      <transformations/>
    </rule>

        ; Rule consider time and queue state.
    <rule id="AA56i10">
      <conditions>
            <nena:QueueState>Active</nena:QueueState>
        <nena:time-period>
          <time dtstart="19970105T083000"
          timestart="2200"
          timeend="0800"
          byweekday="MO,TU,WE,TH,FR"
          dtend="19991230T183000"/>
         </nena:time-period>
      </conditions>
      <actions>
            <priority>5</priority>
        <nena:route>

<nena:recipient>sip:answering-machine@home.foo-bar.com
          </nena:recipient>
        </nena:route>
      </actions>
      <transformations/>
    </rule>
  </ruleset>
```



One Nation 9-1-1 One Number

#### 4.3.2.4 Namespace

This document defines (see section 11.1.5) and uses the NENA URN namespace "urn:nena:xml:ns:policy.policy-v1".

## 4.4 LoST

LoST (RFC 5222 [61]) is the protocol that is used for several functions:

- Call routing: LoST is used by the ECRF as the protocol to route all emergency calls both to[16] 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 [61]. 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.

### 4.4.1 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 Services Routing Proxy (ESRP) to support routing of emergency calls. The ESRP passes the Service URN and location information[17] 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 (e.g.) 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 URI. 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 5.3 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 5.2.1.1). The response of the ECRF is determined by provisioning of the service boundary layers, which specify

[16] 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.

[17] 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.

the URN they apply to (see Section 5.3.1 ). Thus, ECRFs (and ESRPs) 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.

### 4.4.2 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 5.3) to determine if the location is suitable for use (specifically, if the location can be used to accurately route the call and dispatch responders). "LVF Valid" means a location that returns a valid indication (i.e. no fields in the <invalid> list) from an LVF query with the location. 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). Note that since the LVF (and the ECRF) contain a number of fields not normally considered part of a 9-1-1 valid location, it is possible to send a location which may be missing fields that normally ARE considered part of a valid location, and yet get a valid result from an LVF query if (and only if) the fields supplied match a single location in the LVF. For example, many postal addresses match exactly one location in the LVF, and yet are not normally considered 9-1-1 addresses. If a location contains a postal community name, but not the actual municipality name, as long as the LVF (and thus the ECRF) can uniquely identify the address as a single dispatchable location, it is considered LVF-valid. When needed, the other fields can be retrieved from the GIS system by doing the same matching, locating the record and retrieving the missing fields.

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.

### 4.4.3 <findService> Request

The "civic" and "geodetic-2d" profiles are baseline profiles defined in RFC 5222 [61]. 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.

ECRF/LVF should expect to receive any of the PIDF-LO elements described in NENA Civic Location Data Exchange Format (CLDXF) [108] document within a civic location.

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, arcband 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:nena:service". ECRF implementations must support "urn:nena:service". The use of such service URNs is dependent on provisioning of service boundary layers in the GIS. NENA service URNs are defined in Section 11.3.

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.

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 5.14.6). The internal ECRFs and LVFs (see Section 5.14), 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.

### 4.4.4 <findService> Response

LoST servers can 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 domain name 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 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 “urn:nena:service:additionalData”. LoST servers should return SIPS and HTTPS URIs in addition to the SIP and HTTP (where 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.

Responses from ECRFs probably 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.

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 [61] 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:nena: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 would be “911”.

If the ECRF is configured to allow it, a requesting entity can obtain the boundary of the service area handled by the requested service, returned in the <serviceBoundary> element of <mapping>. This is most useful for mobile devices that use geodetic coordinates since they can track their location. When they leave the service area, they can send another <findService> request to determine the

proper service area for their new location and avoid re-querying the ECRF as long as they are within the returned boundary.

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 more than a few points when the device is very close to an edge where the mapping will be different.

Because a service boundary is not needed to initiate an emergency call, and because a complex boundary may be quite large, it is recommended that an ECRF 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.

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. A response with only <valid> and/or <unchecked> elements should be entered into the LIS.

Provisioning of the LoST server is defined by Section 4.6 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. The provisioning includes a flag in the Centerline layer that specifies whether any house number in the range is considered valid (SSNR), or if the house number must appear in the Site/Structure data (SSVAL) to be considered valid. Depending on the

LVF implementation, the outcome of this check may result in one or more civic elements being returned as invalid or unchecked.

### 4.4.5 getServiceBoundary

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

### 4.4.6 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:nena: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.

### 4.4.7 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).

- <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 could not find an answer to the query. This would occur if the authoritative server cannot find the location and has no applicable default route, 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" (or for ECRFs inside the ESInet, "urn:nena:service").

### 4.4.8 Lost Query Examples

#### 4.4.8.1 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>
```

A <findServiceResponse> Response to 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 info:

```
<?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 partial-formed query:

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

```
<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 revision of this document.

## 4.5 Event Notification

Events are communicated within and between ESInets using the SIP SUBSCRIBE/NOTIFY mechanism described in RFC 3265 [17]. ESInet functional elements may need to accept or generate events to outside elements using different asynchronous event notification mechanisms, which would need to 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 3265.

## 4.6 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 Map Database 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, 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. A 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 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 data structure for the SI is defined in Appendix B. The GIS Data Model 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 [130] describes a layer replication interface service for geospatial databases using the Web Feature Service (WFS) [129] and the ATOM protocol (RFC 4287 [131] and RFC 5023 [132]). 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, resolution feed, and a replication feed. The SI layer replication interface is patterned after the replication feed described within OGC 10-069r2.

Note: OGC 10-069r2 is an OGC Public Engineering Report, not a standard. OGC 10-069r2 is not believed to be definitive enough to enable multiple interoperable implementations. A future OGC specification or a future revision of this document is needed to describe the protocol definitively. As with any standardized interface in this document; implementations may provide alternatives to the SI interface in addition to the standard interface defined in this section. A standard NENA schema for WFS as used in the i3 SI layer replication protocol will be provided in a future revision of this document.

## 4.7 Discrepancy Reporting

Any time there is a database, errors or discrepancies may occur in the data. There must be a discrepancy report (DR) function to notify agencies and services (including the BCF, ESRP, ECRF, Policy Store and LVF) when any discrepancy is found. The discrepancy reporting audience is anyone who is using the data and finds a problem. Some of the places discrepancies could occur include:

- The LIS needs to file a Discrepancy Report on the LVF
- The ECRF/LVF may be receiving data from another ECRF/LVF and thus will file a DR on its upstream provider
- The ECRF/LVF needs to file a DR on the GIS
- The ESRP needs to file a DR on the owner of a routing policy (PSAP, ESRP) that has a problem
- The PSAP needs to file a DR on an ESRP if a call is misrouted
- The PSAP needs to file a DR on the GIS when issues are found in a map display
- Any client of an ECRF needs to file a DR on the routing data (which could be a GIS layer problem or something else)
- A PSAP or ESRP needs to file a DR on a LIS
- A PSAP or ESRP needs to file a DR on an ADR/IS-ADR
- A BCF, ESRP or PSAP needs to file a DR on a originating network sending it a malformed call
- Any client may need to file a DR on the ESInet operator
- One PSAP needs to file a DR on another PSAP that transferred a call to it
- A data user may need to file a DR on a data owner due to rights management issues
- A log client (logging entry or query) may need to file a DR on the Logging Service
- Any entity may have to file a DR on another entity due to authentication issues (bad certificate, unknown entity, etc.)
- An ESRP or PSAP may need to file a DR on a Border Control Function
- Any Policy Enforcement Point may need to file a DR on a Policy owner due to formatting, syntax or other errors in the policy

This document provides a standardized Discrepancy Reporting mechanism in the form of a web service. Each database or service agency must provide a Discrepancy Reporting web service. When a discrepancy is reported on an element (such as an ECRF), the web service will be 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 may be a long time elapsed from the sending of the report to receiving the resolution and a call-back mechanism is provided for the responding agency to send the resolution to the reporting agency.

A Discrepancy Report (DR) is sent by the agency reporting the discrepancy to a responding agency and will pass through several phases:

- The reporting agency creates the DR and forwards it to the responding agency
- The responding agency acknowledges the DR report and provides an estimate of when it will be resolved
- The reporting agency may request a status update and receive a response
- The responding agency resolves the DR and reports its resolution to the reporting agency

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

- Time Stamp of Discrepancy Submittal
- Discrepancy Report ID
- Discrepancy reporting agency domain name
- Discrepancy reporting agent user ID
- Discrepancy reporting contact info
- Service or Instance in which the discrepancy exists
- Additional notes/comments
- Reporting Agency's assessment of severity
- Discrepancy Service or Database specifics

For each type of Discrepancy Report there is a specific database or service where the discrepancy originated or occurred. Within the database or service there is a defined block of data specific to the database or service that will be included in the DR and must include:

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

The Agency Locator (Section 5.16) provides the URI to an agency's DR service. For elements (such as an ECRF) that must have a corresponding DR web service, no discovery mechanism is currently specified, and will be addressed in a future revision of this document.

### 4.7.1 Discrepancy Report

The Discrepancy Reporting web service is used by a reporting agency to initiate a Discrepancy Report and includes the following functions:

**DiscrepancyReportRequest**

| Parameter | Condition | Description |
|---|---|---|
| Timestamp | Mandatory | Timestamp of Discrepancy Report |

| Parameter | Condition | Description |
|---|---|---|
| | | Submittal |
| ReportId | Mandatory | Unique (to reporting agency) ID of report |
| ReportingAgency | Mandatory | Domain name of agency creating the report |
| ReportingAgent | Optional | UserId of agent creating the report |
| ReportingContact | Mandatory | vCard of contact about this report |
| ResolutionURI | Mandatory | URI for responding agency to use for responses |
| Service[1] | Conditional | Name of service or instance where discrepancy exist |
| Severity | Mandatory | Enumeration of reporting agency's opinion of discrepancy's severity |
| Comment | Optional | Text comment |
| Discrepancy[2] | Mandatory | Database/Service-specific block |

[1] Each database/service description denotes whether the "Service" parameter is required for that database/service or not, and provides an XML description of the "Discrepancy" parameter content.

[2] In cases of routing discrepancies, the PIDF-LO would be included.

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

**DiscrepancyReportResponse**

| Parameter | Condition | Description |
|---|---|---|
| StatusCode | Mandatory | Status code |

Status Codes

200 Okay No error

522 Unknown Service/Database ("not ours")

523 Unauthorized Reporter

504 Unspecified Error

### 4.7.2 DiscrepancyResolution

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

DescrepancyResolutionRequest

| Parameter | Condition | Description |
|---|---|---|
| ReportId | Mandatory | Unique (to reporting agency) ID of report |
| RespondingAgency | Mandatory | Domain name of agency responding to the report |
| RespondingAgent | Optional | UserId of agent responding to the report |
| RespondingContact | Mandatory | vCard of contact about this report |
| Comment | Optional | Text comment |
| StatusCode | Optional | Status Code |
| Resolution | Mandatory | Database/Service-specific resolution data |

Status Codes

200 Okay No error

5xx Unknown ReportId

5xx Unauthorized Responder

504 Unspecified Error

### 4.7.3 Status Update

A reporting agency may request a status update. The mechanism defined assumes the responding agency 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 includes:

**StatusUpdateRequest**

| Parameter | Condition | Description |
|---|---|---|
| ReportId | Mandatory | Unique (to reporting agency) ID of report |
| ReportingAgency | Mandatory | Domain name of agency creating the report |
| ReportingAgent | Optional | UserId of agent creating the report |
| ReportingContact | Mandatory | vCard of contact about this report |

| Parameter | Condition | Description |
|---|---|---|
| Comment | Optional | Text Comment |

The response to this request includes:

**StatusUpdateResponse**

| Parameter | Condition | Description |
|---|---|---|
| RespondingAgency | Mandatory | Domain name of agency responding to the report |
| RespondingAgent | Optional | UserId of agent responding to the report |
| RespondingContact | Mandatory | vCard of contact about this report |
| EstimatedResponseTimestamp | Mandatory | Estimated date/time when response will be returned to reporting agency or the actual time, in the past when the response was provided. |
| Comment | Optional | Text Comment |
| StatusCode | Optional | Status Code |

Status Codes

200 Okay No error

524 Unknown ReportId

523 Unauthorized Reporter

5xx Resolution already provided

504 Unspecified Error

### 4.7.4 LVF Discrepancy Report

A client of an LVF may report a discrepancy. The most common report is that the LVF claims the location sent in the PIDF-LO is invalid, when the client believes it is valid.

**LVFDiscrepancyReport** is defined as:

| Element | Condition | Description |
|---|---|---|
| Location | Mandatory | Location queried |
| Service | Mandatory | Service URN queried |



One Nation 9-1-1 One Number

| Element | Condition | Description |
|---|---|---|
| LocationValidation | Mandatory | Validation Response |
| Discrepancy | Mandatory | BelievedValid, OtherReport |

**LVFDiscrepancyResponse** is defined as:

| Element | Condition | Description |
|---|---|---|
| ValidationResponse | Mandatory | EntryAdded, NoSuchLocation, OtherResponse |

### 4.7.5 Policy Discrepancy Report

A client of a Policy may report a discrepancy. The most common report is that the Policy Query returns an invalid Policy from the Policy Store.

**PolicyDiscrepancyReport** is defined as:

| Element | Condition | Description |
|---|---|---|
| PolicyName | Mandatory | The name of the policy |
| Agency | Mandatory | The agency whose policy is requested. Must be a domain name or URI that contains a domain name |
| RetrievePolicyResponse | Mandatory | The Response received from the Policy Retrieve Request as shown in 4.3.1 |

**PolicyDiscrepancyResponse** is defined as:

| Element | Condition | Description |
|---|---|---|
| ValidationResponse | Mandatory | Policy Added, Policy Updated, No Such Policy, Other Response |

### 4.7.6 LoST Discrepancy Report

To be supplied in a future revision of this document.

### 4.7.7 ECRF Discrepancy Report

To be supplied in a future revision of this document.

### 4.7.8 BCF Discrepancy Report

To be supplied in a future revision of this document.

### 4.7.9 Log Discrepancy Report

To be supplied in a future revision of this document.

### 4.7.10 PSAP Call Taker Discrepancy Report

To be supplied in a future revision of this document.

### 4.7.11 Permissions Discrepancy Report

To be supplied in a future revision of this document.

### 4.7.12 GIS Discrepancy Report

To be supplied in a future revision of this document.

# 5 Functions

## 5.1 Border Control Function (BCF)

A BCF sits between external networks and the ESInet and between the ESInet and agency networks. All traffic from external networks transits a BCF.

### 5.1.1 Functional Description

The BCF comprises several distinct elements pertaining to network edge control and SIP message handling. These include:

- Border Firewall
- Session Border Control

It is imperative that the BCF supports 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-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 Community 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;

5) Adhere to the default deny principle.

Please refer to NENA 04-503 [101] 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.

The following primary functions are related to the SBC 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 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 5.1.2.
- 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.
- 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).
- 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 shall optionally support transcoding. For example, the SBC component may transcode Baudot tones to RFC 4103 [117] real time text. See Section 4.1.8.3.
- Encryption: The SBC component of the BCF shall support encryption (AES on TLS) for calls that are not protected entering the ESInet.

Additionally, the SBC component of the BCF performs 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.

*Media encryption and decryption*

1. Encryption and decryption of media streamed (e.g., IPsec).

*B2BUA for UAs that do not support Replaces*

- The SBC component may include a B2BUA function for 9-1-1 calls where the caller does not indicate support for the Replaces operation. See Section 5.9.1.

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.

### 5.1.2 Interface Description

The BCF supports SIP interfaces upstream and downstream per Section 4.1. BCFs must support ROHC [144]. The BCF, as the first active SIP element in the path of an emergency call, adds the Call Identifier, Incident Tracking Identifier and Resource-Priority (if not already present) to the call. These identifiers must be added to the initial message of a dialog forming transaction (INVITE) or the MESSAGE method associated with a non-human-initiated call. The identifiers should be added to all other SIP messages processed by the BCF. 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 include a "NENA-source" parameter in the Via header that it inserts 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 NENA-source parameter is formatted as follows: <unique source-id>@<domain name of BCF> (e.g., "a7123gc42@sbc22.example.net").

When the downstream element identifies a source as a "bad actor", it signals the BCF which source is misbehaving by sending it a BadActorRequest that contains the sourceId from the NENA-source parameter that was included in the Via header of the incoming INVITE message. 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 filter out subsequent calls from that source until the attack subsides.

The bad actor request/response is a webservice operated on the domain mentioned in the parameter.

**BadActorRequest**

| Parameter | Condition | Description |
|---|---|---|
| sourceId | Mandatory | sourceId from a NENA-source parameter |

**BadActorResponse**

| Parameter | Condition | Description |
|---|---|---|
| statusCode | Mandatory | Status Code |

Status Codes

200 Okay No error

101 Already reported

513 No such sourceId

514 Unauthorized

504 Unspecified Error

BCFs that anchor media must implement the Session Recording Client interface defined by SIPREC [153]. Provisioning may control whether the BCF logs media.

#### 5.1.2.1 CallSuspicion

The BCF may be able to 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 bad call show up to having a good call dropped. The behavior of downstream elements (ESRPs for example) may be affected by the determination of the BCF. For this purpose, the BCF attaches a parameter to the Via header it inserts on the call. The parameter "NENA-CallSuspicion" is a 0-100 score of call suspicion where 0 is least suspicious and 100 is most suspicious.

### 5.1.3 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.

### 5.1.4 Operational Considerations

In order to withstand the kinds of attacks anticipated, BCFs at the edge of the ESInet should be provisioned with capacity, both aggregate uplink bandwidth and BCF processing capacity larger

than the largest feasible DDoS attack. As of this revision, that capacity is approximately 6-8 Gigabits of mitigation.

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. It is essential that all BCF support organizations 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.

## 5.2 Emergency Service Routing Proxy (ESRP)

### 5.2.1 Functional Description

#### 5.2.1.1 Overview

The Emergency Service Routing Proxy (ESRP) is the base routing function for emergency calls for i3. As described in NENA 08-002 [100], 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 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 call taker or set of call takers.

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 URI. 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 (possibly) rewritten, a Via header added, and in some cases, additional manipulation of the SIP messages. To do its job, the ESRP has interfaces to the ECRF for location based routing information, as well as various event notification sources to gather state, which is used by its Policy Routing Function (PRF).

For typical 9-1-1 calls with a Request URI starting with "urn:service:sos" received, the ESRP will:

1) Evaluate an origination policy "rule set" 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[18];
3) Evaluate a termination policy rule set for that URI using other inputs available to it such as headers in the SIP message, time of day, PSAP state, etc.

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).

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 BCF to an ESRP and be subject to the same security and policy routing as regular 9-1-1 calls. Such calls would normally not have a Geolocation header, but would arrive on a different queue, have a different origination policy, would not query an ECRF and would use a fixed URL for "Normal-Next Hop".

For calls forwarded by a PSAP to a responder with a Request URI of "urn:nena:service:responder.*" and a Route header containing the responder URI, the ESRP uses the domain of the Route header to choose an origination policy and evaluates it per 1-3 above. 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 are encouraged to 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 termination policy for the Route header in this circumstance forward the call to the domain specified in the route header with no further processing.

An ESRP is usually the "outgoing proxy server" for calls originated by the PSAP. The ESRP would route calls within the ESInet, and would route calls to destinations outside the ESInet through an appropriate gateway or SIP trunk to a PSTN or other carrier connection. Call-backs to the original caller are an example of such outgoing calls to external destinations. No policy rule set evaluation is used for outgoing calls. While an ESRP could be an incoming proxy server for non-emergency calls, such use is beyond the scope of this standard.

#### 5.2.1.2 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, it can have one or many sources taking calls off the queue. All queues defined in this document are normally First In First Out. A unique SIP URI identifies a queue. A queue is normally managed by an ESRP. 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 endpoint such as a call taker or IMR. As such, all call queues are "ingress" queues, conceptually on the input side of an ESRP. In cases where more than one dequeuer exists for

[18] The ECRF query is invoked as part of rule evaluation. A given ruleset need not invoke an ECRF query, but all ESRPs must implement the capability to query an ECRF

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 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.

In practice, some proxy servers may be simple RFC 3261 [12] 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 and dequeue 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 will maintain a QueueState notifier, and track the number of calls in queue for the queues that it manages. ElementState overrides QueueState (if the Element is Down, the queue is Inactive).

#### 5.2.1.3 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 3265[17] is used to report QueueState. The event includes the URI of the queue, the current queue length, allowed maximum length and a state enumeration including:

- Active: one or more entities are actively available or are currently handling calls being enqueued
- Inactive: no entity is available or actively handling calls being enqueued
- Disabled: The queue is disabled by management action and no calls may be enqueued
- Full: The queue is full and no new calls can be enqueued on it.
- 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".

QueueState need not be implemented on simple routing proxy or when queue length is 1 and only one dequeuer is permitted.

**Event Package Name**: nena-QueueState

**Event Package Parameters**: None

**SUBSCRIBE Bodies**: standard RFC 4661 [127] + 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/vnd.nena.queuestate+xml

| Parameter | Condition | Description |
|---|---|---|

| Parameter | Condition | Description |
|---|---|---|
| queue | Mandatory | SIP URI of queue |
| queueLength | Mandatory | Integer indicating current number of calls on the queue. |
| maxLength | 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 202 Accepted.

**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:** No specific action required.

**Handling of Forked Requests:** Forking is not expected to be used with this package.

**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 [112]. 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:** No special handling is required.

Race conditions exist where 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 where the current queue length is equal to or greater than the allowed maximum queue length will have an error (486 Busy Here) returned by the dequeuer. An ESRP that dequeues a call, sends it to a downstream entity and receives a 486 in return must be able to either re-enqueue the call (at the head of the line) or send it to another dequeueing entity. 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 entities point of view. Network state 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 [112] to control the rate of Notification.

#### 5.2.1.4 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 will manage a queue where it is the only dequeuer, and this web service will not be needed. When there is more than one dequeuer, they 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 will 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 will attempt to fairly distribute calls to the set of entities with the same DequeuePreference measured over tens of minutes.

**DequeueRegistrationRequest**

| Parameter | Condition | Description |
|---|---|---|
| queue | Mandatory | SIP URI of queue to register on |
| dequeuer | Mandatory | SIP URI of dequeuer (where to send calls) |
| expirationTime | Mandatory | Requested time in seconds this registration will expire |
| dequeuePreference | Optional | Integer from 1-5 indicating queuing preference. |

**DequeueRegistrationResponse**

| Parameter | Condition | Description |
|---|---|---|
| expirationTime | Mandatory | Time in seconds this registration will expire. |
| statusCode | Optional | Status Code |

Status Codes

200 Okay No error

506 Bad queue

507 Bad dequeuePreference

508 Policy Violation

504 Unspecified Error

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 of the ESRP. A request expirationTime of zero is a request to deregister. The entity managing the queue has a policy 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.

#### 5.2.1.5 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 two or more policy rule sets, whose syntax is described in Section 4.3.2: One set determined by the queue the call arrives on, the other is determined by the result of an ECRF query with the location of the caller.

The PRF in an ESRP accepts calls directed to a specific queue URI. From that URI, it extracts its own "OriginationPolicy" from its Policy Store for that URI and executes the rule set. The rules normally include at least one condition LoSTServiceURN(<urn>) where <urn> is a service URN (either urn:service:… or urn:nena:service:…). Upon encountering the LoSTServiceURN condition, the PRF queries its (configured) ECRF with the location received with the call using the <urn> parameter in the action. The resulting URI is a variable called "Normal-NextHop". The PRF extracts a "TerminationPolicy" from its Policy Store associated with the domain of Normal-NextHop and executes the rule set associated with that policy. The rules normally include the action "Route". The PRF forwards the call to the route. It would be common for the route of a 9-1-1 call intended for a PSAP in a normal state to be identical to the "Normal-NextHop" URI, that is, if the ECRF query returned "sip:psap1@example.com", then the TerminationPolicy rule set for "sip:psap1@example.com" would have a "Route(sip:psap@example.com)" or a "Route(Normal-NextHop)", which is equivalent, if the state of psap1 is nominal. If the Policy Store the ESRP uses does not contain a TerminationPolicy rule set for the Normal-NextHop URI, the ESRP will route the call directly to that URI.

The destination of a Route action is usually the URI of a queue, but a simple proxy server can be the next hop. 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 [43], which plays an announcement (in the media negotiated by the caller) and potentially accepts responses via DTMF, KeyPress Markup Language [195] or other interaction styles.

Other Actions that may occur in a Termination-Policy 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 yields a value for NextHop, the rule with the highest priority prevails.

Usually, there is a "default" rule for use when everything is in normal status. Most calls will route via this rule, for example "IF True THEN Route (Normal-NextHop) {10}". 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 default 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 is established for that route, with one dequeueing 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 they arrive on.

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 low priority rule for overload for 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.

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 (and thus no termination policy rule set is used). In such a case, the origination policy rule set would determine NextHop. Rules can determine the priority of multiple queues feeding calls to the ESRP. PSAP ESRPs may dequeue for multiple call queues managed by it or other entities, placing them on internal queues for call takers.

#### 5.2.1.6 ESRPnotify Event Package

The ESRP sends a Notify for this event when the PRF encounters a Notify action. It is used to inform other agencies or elements about conditions in an incoming call they may be interested in. For example, a call that contains an Additional Data block may have a telematics dataset that indicates a severe injury. The rule set may issue the ESRPnotify event to a helicopter rescue unit to inform them that their services may be needed. The ESRPnotify event is defined as follows:

**Event Package Name**: nena-ESRPnotify

**Event Package Parameters**:

| Parameter | Condition | Description |
|---|---|---|
| Normal-NextHop | Mandatory | URI of downstream entity occurring in a Termination-Policy |
| ESRPEventCode | Mandatory | Enumeration of event codes. May occur more than once |

**SUBSCRIBE Bodies**: standard RFC 4661 [127] + 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/vnd.nena.ESRProute+xml

The ESRPnotify NOTIFY contains a Common Alerting Protocol (CAP) message, possibly wrapped in an EDXL wrapper. The <area> element of the CAP message contains the location of the caller in the Geolocation header, although <area> is always location by value. The CAP message is in the body of the NOTIFY, with MIME type application/common-alerting-protocol+xml.

**ESRPnotify**

| Parameter | Condition | Description |
|---|---|---|
| esrpCAPmessage | Mandatory | CAP Message for this event |
| esrpCondition | Mandatory | Rule and values that triggered the event |

Note: If the URI in the Notify action in a rule contains a service URN, then the CAP message is sent to entities whose service boundaries intersect the location of the caller where the service URN matches that in the Notify action. In such a case, a SIP MESSAGE is used, rather than a SIP NOTIFY.

The <identifier> is determined by the ESRP, and must be globally unique. The identifier in the CAP message is not the same as the Call Identifier assigned in the ESInet, but the log contains the record that relates the two.

The <sender> is the NextHop URI (i.e., the downstream entity whose rules invoked the Notify).

The <addresses> element contains the URIs of the subscribers to the event that are being notified.

An <info> element must be included. The element must contain an <event code>. The <valueName> must be "NENA-EsrpNotify". 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 0. The <event category> is determined from the registry: each event code has a corresponding category

<urgency>, <severity> and <certainty> are copied from the parameters in the Notify action from the rule.

The SIP message that initiated the event must be sent in the CAP message in a <parameter> element with a value name of <sipMessage>[19]. If there are Call-Info header fields containing Additional Data, they must be sent in the CAP message in a <parameter> element with a <value name> of ADDLDATA. The URI(s) or MIME object(s) containing the Additional Data is in the <value> element.

A digital signature should be included in the CAP message. The message should not be encrypted. TLS may be used on the SIP MESSAGE transmission to encrypt the message.

[19] There may be some privacy concerns in sending all SIP message content to some event recipients. Policy at the ESRP may filter the header content to some recipients.

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

**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 if 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 202 Accepted.

**Notifier Generation of NOTIFY Requests:** When the Notify (ESRProuteEventCode) action is present in the rule that determines routing, send NOTIFY to any subscriber requesting that notification (based on the Normal-NextHop whose policy is being evaluated and the ESRProuteEventCode present in the action.

**Subscriber Processing of NOTIFY Requests:** No specific action required.

**Handling of Forked Requests:** Forking is not expected to be used with this package.

**Rate of Notification:** A notification for each call/event handled by the ESRP could be sent. Rate controls [112] may be used to limit Notifications.

**State Agents:** No special handling is required.

#### 5.2.1.7 Processing of an INVITE transaction

When the ESRP receives an INVITE transaction it first evaluates the Origination rule set for the queue the call arrived on. If a LoSTServiceURN condition is encountered it looks for the presence of a Geolocation header. If present, the ESRP evaluates the header and extracts the location in the Geolocation header [10]. Each ESRP must be capable of receiving location as a value or a reference, and must be provisioned with credentials suitable to present to all LISs in its service area to be able to dereference a location reference using either SIP or HELD.

The ESRP must be able to handle calls with problems in location. This can occur if the call is originated by an element outside the ESInet, the call is to an emergency service URN, and there is no Geolocation header. This also occurs 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 location. In all such cases the ESRP must make a best effort to determine a suitable default location to use to route the call. The call source, IP address of the caller or other information from the INVITE may be used to determine the best possible default location. It is felt that the earlier in call processing that bad or missing location is determined, the more likely the ESRP will have information needed to get the best possible default location, and downstream entities will be in a worse position to do that.

The ESRP then queries its local (provisioned) ECRF with the location, using the service URN specified and the value of the RequestURI in the LoSTServiceURN condition parameter. For example, the originating ESRP receiving an emergency call from outside the ESInet 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:nena:service.sos.psap”. The ECRF returns a URI for that service. Calls to an administrative number do not have location and are mapped by a provisioned table in the ESRP from the called number to a URI.

The ESRP retrieves the terminating policy rule set for the URI. The PRF evaluates the rule set using the facts available to it such as PSAP state, time of day, queue state, information extracted from the INVITE, etc. The result is a URI of a queue. The ESRP attempts to forward the call to the URI, using the DNS to translate the URI into an IP address. DNS may provide alternate IP addresses to resolve the URI. Normal SIP and DNS processing is used to try these alternate IP addresses. Should no entity respond, the ESRP must provide the call with a provisioned treatment such as returning busy. Note that normally the state of the downstream elements that would appear in the URI is reported to the ESRP and the rule set would use that state to specify an alternate route for the call.

Calls that are received by an ESRP which originate inside the ESInet are routed per normal SIP routing mechanisms. Calls to E.164 telephone numbers not otherwise provided for in the ESRP provisioning must be routed to a provisioned gateway or SIP trunk interconnected to the PSTN.

#### 5.2.1.8 Processing a BYE Transaction

An ESRP processes BYEs per RFC 3261 [12].

#### 5.2.1.9 Processing a CANCEL transaction

An ESRP processes 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.

#### 5.2.1.10 Processing an OPTIONS transaction

An ESRP processes OPTIONS transactions per RFC 3261. 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.

### 5.2.2 Interface Description

#### 5.2.2.1 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, or a BCF between a PSAP and the ESRP for calls sent by the PSAP. The upstream SIP call interface for the originating ESRP must only assume the minimal methods and headers as define in Section 4.1.1 but must handle any valid SIP transaction. All other ESRPs must handle all methods and SIP headers. 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 for calls sent to “urn:service:sos”.

The upstream SIP interface is also used for calls originated inside the ESInet, where the ESRP is the outgoing proxy for a PSAP. Calls originated in the ESInet and destined for agencies within the ESInet are routed by the ESRP using normal SIP routing methods. Calls originated in the ESInet and destined for external termination (such as call backs) are routed to gateways or SIP trunks terminated by a carrier.

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.

#### 5.2.2.2 Downstream Call Interface

The ESRP downstream call interface typically faces a downstream ESRP for all but the terminating ESRP, which typically faces user agents. 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 headers noted in Section 4.1.2 permitted by the relevant RFCs to be added by proxy servers. The INVITE transaction exiting the ESRP must include a Via header specifying the ESRP. It must include a Route header. The Request URI remains "urn:service:sos"[20] (although the ESRP may not depend on that; a call presented to an ESRP that is not recognized as, for example, a call to an admin line, will be treated as an emergency call and its occurrence logged) and it replaces the top Route header with the next hop URI (this is described in RFC 6881 [59]). The ESRP adds History-Info header and Reason parameter headers per Section 4.1.7 using the cause code specified in the Route action if cause is specified (which it would be for a diverted call).

A call entering the ESInet is initially assumed to be a new Incident. Thus, the first ESRP in the path adds a Call-Info header field, if one is not already present, with a purpose parameter of "nena-IncidentId" and a new Incident Tracking Identifier per Section 3.1.6. The ESRP also creates a new Call identifier (Section 3.1.5) and adds a Call-Info header field with a purpose parameter of "nena-CallId" if one is not already present.

The downstream interface must implement TCP/TLS towards downstream elements, but must be capable of fallback to UDP. SCTP support is optional. No ESRP may remove headers received in the upstream call interface; all headers 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 call back. A call back would be accepted on its downstream interface and sent towards the origination network on its upstream interface.

#### 5.2.2.3 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 |
|---|---|

[20] 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.



One Nation 9-1-1 One Number

| URN | Use |
|---|---|
| urn:nena:service:sos.psap | Route calls to primary PSAP |
| urn:nena:service:sos.level_2_esrp | Route calls to a second level ESRP (for an example, a state ESRP routing towards a county ESRP) |
| urn:nena: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). |
| urn:nena:service:sos.call_taker | Route calls to a call taker within a PSAP |

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 5.2.1.4). The specific service URN used by an ESRP is specified in its origination routing policy (see Section4.3.2.1.9). Any URN in the "urn.service.sos" or "urn:nena.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 nena 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:nena:service:additionalData" service URN when the relevant rule set specifies an element in that structure. The same location used for the location-based route is used for the Additional Data query.

#### 5.2.2.4 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 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[21]. 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 persistent TCP and TLS connections to LISs that it has frequent transactions with. A suggested value for "frequent" is more than one transaction per day.

#### 5.2.2.5 Additional Data Interfaces

The ESRP must implement mechanisms for retrieving Additional Data [143]. These services may be invoked when the ESRP receives a call with a CallInfo [12] header field having a "purpose" starting with "EmergencyCallData"[22], or from a PIDF-LO with an appropriate <provided-by> element and

[21] 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.
[22] E.g., purpose=EmergencyCallData.ProviderInfo

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", passed by value using the Content Identifier or by reference with an HTTPS URI, may occur 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.

Additional Data is accessed via the following mechanisms:

- Through dereferencing URI(s), added to the Call-Info header field by the device, originating network or service provider handling the call. Each Additional Data URI is dereferenced against its respective target ADR to return the stored caller data.
- By querying an "Identity Searchable Additional Data Repository" (IS-ADR) with the identity obtained from Caller's From or P-Asserted-Identity headers to retrieve an XML document containing any available Additional Data[23].

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 that location. This URI may be dereferenced by the ESRP on an ADR to drive PRF rules. Any returned Additional Data URI may be added in a Call-Info header field such that it can be referenced 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 will return 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 11.31 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 where there is more than one resident and each supplies its own Additional Data blocks. 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 revision of this document.

[23] Refer to section 5.11.1 Identity Serchable Additional Data Repository (IS-ADR) for further detail on the interfaces exposed by this functional element.

#### 5.2.2.6 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 it expects to receive calls from. The 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.

#### 5.2.2.7 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.

#### 5.2.2.8 Logging Interface

The ESRP must implement a logging interface per Section 5.13. 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 log event records for these are provided in Section 5.13.3.

#### 5.2.2.9 AbandonedCall Event

The ESRP uses the AbandonedCallEvent to notify a PSAP that a call was started, but then cancelled prior to the PSAP knowing the call occurred.

**Event Package Name**: nena-AbandonedCall

**Event Package Parameters**: None

**SUBSCRIBE Bodies**: standard RFC 4661 [127] + 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/vnd.nena.AbandonedCall+xml

| Parameter | Condition | Description |
|---|---|---|
| Invite | Mandatory | Content of INVITE message |
| InviteTimestamp | Mandatory | Timestamp call was received at ESRP |

| Parameter | Condition | Description |
|---|---|---|
| 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 202 (Accepted).

**Notifier Generation of NOTIFY Requests:** When the ESRP receives a CANCEL for a call, and it is not certain that the downstream entity that should get that call received an INVITE for the call, a new NOTIFY is generated, adhering to the filter requests.

**Subscriber Processing of NOTIFY Requests:** No specific action required.

**Handling of Forked Requests:** Forking is not expected to be used with this package

**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.

### 5.2.3 Data Structures

The ESRP maintains an ElementState structure for its own state, and an ElementState structure for every downstream element it serves.

If the ESRP manages queues, it maintains a QueueState structure for each queues it manages, including the states of the entities registered to enqueue and dequeue calls from the queue, the overall queue state, the number of calls in queue, the maximum number of calls allowed, and the current queue state.

The ESRP constructs Additional Data structures when the relevant rule set mentions elements from these structures.

### 5.2.4 Policy Elements

The ESRP uses an Origination-Policy rule set for each queue it manages. The ESRP must have access to the appropriate Termination-Policy ruleset for every URI that the ECRF can return in response to a service query made by the ESRP (Normal-NextHop).

The enqueuer policy specifies which entities can enqueue calls on the queue.

The ESRProuteEvent Policy determines which entities may subscribe to the ESRProute Event (see Section 5.2.1.6).

The QueueState policy determines which entities may subscribe to the QueueState event.

The ElementState policy determines which entities may subscribe it its ElementState event.

The DequeueRegistration policy determines which entities may subscribe to the DequeueRegistration event.

Note: Specific policy document structures will be specified for each of the above in a future revision of this document.

### 5.2.5 Provisioning

The ESRP is provisioned with:

- The queues it manages;
- The queues it dequeues from;
- 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 URI of a default route PSAP that takes calls when a route cannot be determined.

### 5.2.6 Roles and Responsibilities

An ESRP may be operated by a State, Regional or local 9-1-1 Authority. A terminating ESRP may be operated by a PSAP. The ESRP operators for non-originating ESRPs must supply a rule set for the upstream ESRP.

### 5.2.7 Operational Considerations

If a routing rule depends on Additional Data dereferenced from a server not under the control of the 9-1-1 Authority, it could add significant delay to processing the rule and may not be reliable.

Additional considerations will be provided in a future revision of this standard.

## 5.3 Emergency Call Routing Function (ECRF) and Location Validation Function (LVF)

In i3, emergency calls will be routed to the appropriate PSAP based on the location of the caller[24]. 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

[24] 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.

and dispatch prior to the call being placed. We refer to this as having a "valid" location for the call[25]. 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 [61]. The primary validation is accomplished as locations are placed in a LIS. 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 [4]). Periodic re-validation of stored location is also recommended [59][26].

ECRFs and LVFs are queried using the LoST protocol (see Section 4.4). 9-1-1 Authorities provide authoritative ECRFs and LVFs both inside and outside ESInets. Other entities, such as origination 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 origination 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.

### 5.3.1 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 Services 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.

[25] 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.

[26] Short periods (days or a few weeks) allows 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.

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 [168]) 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 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.

### 5.3.2 Interface Description

#### 5.3.2.1 Routing Query Interface

The ECRF and LVF query interface implements the LoST [61] protocol as described in Section 4.4.

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, he 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 B). 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. Theoretically, 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 (that is 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 is 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).

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 (for example, 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 11.31.

LoST can return a service boundary in the response. 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. Any given boundary returned in a LoST response (by value or by reference) need not represent the full extent of the provisioned/actual service boundary, but may be a simplification that does not exceed the provisioned boundary. Such techniques may reduce bandwidth consumption and compute load on the device, and should be considered by ECRF implementations.

If the deployment strategy envisioned in this document were implemented, an external (outside the ESInet) ECRF would map queries for "urn:service:sos" to state level ESInets, and thus state ESRPs. The boundary returned would be a state boundary, or subset of it as described above. Neither ECRFs nor LVFs are required to return service boundaries.

#### 5.3.2.2 Validation Interface

RFC 5222 [61] section 8.4.2 states that the inclusion of location validation is optional, and subject to local policy. NENA i3 requires that all LoST server implementations, deployed as an LVF, 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[27]

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 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 where 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.

[27] Recurse to an LVF may not be desirable since the LVF is not a real time element.

#### 5.3.2.3 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). A SI layer replication interface, as described in Section 4.6, 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 on-line, 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.

#### 5.3.2.4 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.

#### 5.3.2.5 Logging Interface

The ECRF/LVF must implement a logging interface per Section 5.13. 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 provisioning and synchronization messages and actions. Specific LogEvent records for these are provided in Section 5.13.3.

#### 5.3.2.6 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.

#### 5.3.2.7 Service State

The set of ECRFs and LVFs 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.

### 5.3.3 Data Structures

#### 5.3.3.1 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 the ECRF will represent the geographic service boundary in a manner that allows the association of a given address with the service boundary it is located within. 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 accept location information conforming to U.S. addressing standards defined in CLDXF [108] and its eventual Canadian equivalents.

#### 5.3.3.2 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 ECRF/LVF, but they all supply the same resultant URI. ECRF/LVFs can refer or recur 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 return the same response.

#### 5.3.3.3 Service Boundaries

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.

For each service URN supported by an ECRF/LVF, one or more layers will provide polygon sets associated with URIs[28]. 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 with the service URN attribute matching that provided in the LoST query containing the location, and returning the URI attribute of that polygon set. If the proffered location is a shape, that shape may overlap more than one service boundary. The response in that case is determined by an algorithm in the ECRF/LVF,

[28] Multiple URIs each with a different scheme may be returned from an ECRF query

which could be, for example, greatest area of overlap, but is not otherwise specified in this document.

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 (see Appendix B). 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[29]. In the case where a location is a shape, rather than a point, and there are more than one site/structures partially or completely within that shape, the ECRF returns all of the Additional Data URIs associated with those site/structures[30].

A service boundary is not required to be returned for a query. When a civic address is provided and the service boundary is simple (such as a municipality or a state) the ECRF should return that information. If the service boundary is complex it is recommended that the ECRF not return a service boundary.

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 municipality boundary.

#### 5.3.3.4 Routing Data – URI Format

For an end-to-end IP network where 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 URI may identify a PSAP, or an ESRP that will forward calls to the appropriate PSAP. The source of the query and/or the service URN determines which URI is returned. URI format is described in RFC 3986 [163]. 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 information.

#### 5.3.3.5 Validation Data

The LVF uses the same data provided to the ECRF as described in Section 5.3.3.1 above.

[29] The additional data contain the civic address to which they refer, so a geodetic querier can determine to which address the response refers.

[30] 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



One Nation 9-1-1 One Number

### 5.3.4 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 GISs via separate SIs.

In some local GISs, for convenience, the 9-1-1 Authority may provide data that extends beyond the service boundary of the PSAPs within their jurisdiction. Non-authoritative data must not be sent to the ECRF/LVF.

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 meters. Gaps or overlaps that are smaller that 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 uses of the GapOverlap event. All 9-1-1 Authorities who 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) where 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 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.

The GapOverlap event is defined as follows:

**Event Package Name**: nena-GapOverlap

**Event Package Parameters**: none

**SUBSCRIBE Bodies**: standard RFC 4661 [127] + extensions filter specification may be present

**Subscription Duration** Default 24 hour. 1 hour to 96 hours is reasonable.

**NOTIFY Bodies**: MIME type application/vnd.nena.GapOverlap+xml

| Parameter | Condition | Description |
|---|---|---|
| Agency | Mandatory | URI of Agency with gap/overlap. Will be repeated at least twice |

| Parameter | Condition | Description |
|---|---|---|
| Layer | Mandatory | Enumeration of layer where 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 202 Accepted.

**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 is not expected to be used with this package.

**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.

### 5.3.5 Replicas

An ECRF/LVF is essentially a replica of a subset of the layers of one or more source GISs. 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 that permits the ECRF/LVF to do so, and the policy may restrict which entities it may provide replication data to. The ECRF/LVF also has a policy that defines who it will provide data to. If the ECRF/LVF provides a replica service, the interface is the layer replication service as described in Section 4.6. In this case, the ECRF/LVF is the server-side, as opposed to the client interface it must provide towards the SI(s) it receives data from.

### 5.3.6 Provisioning

The ECRF/LVF is provisioned with

- A set of layers from one or more SIs.
- The domains it may accept queries from, if its use is restricted.

To maximize the probability of getting help for any kind of emergency by 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[31]. 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.

### 5.3.7 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. NENA therefore expects that 9-1-1 Authorities will be responsible for inputting the authoritative data for their jurisdiction in 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.

### 5.3.8 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/origination 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[32]. 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.

[31] 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.

[32] 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.

For example, a local ECRF may have a SI to another local ECRF, a regional ECRF may have a SI to all the local ECRFs in its area, a state ECRF may have a SI to all of the regional ECRFs and an access network provider may have an ECRF that has a 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 are reachable from within any ESInet. Since it is not possible that all entities that need to access a LVF will have one in their local domain, a LVF must be accessible from the Internet[33]. 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. Ideally, origination 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 EIDDs related to calls.

LVF elements are based on the LoST server architecture and use the LoST protocol [61]. 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, needs to be able to reach out to other ECRF/LVFs in case of missing data, or in the case where 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/origination networks that use an

[33] 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.



One Nation 9-1-1 One Number

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 origination 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.

### 5.3.9 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:nena:service:sos.*") and other internal services such as "urn:nena:service:agencyLocator". 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.

### 5.3.10 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.

## 5.4 Spatial Interface (SI)

A SI provides an interface between an authoritative copy of GIS data and functional elements within an ESInet such as an ECRF and LVF. A SI layer replication interface is used to maintain copies of GIS layers that drive call routing and location validation within an NG9-1-1 system. In addition, one or more copies of that data can also be maintained on other services using the SI layer replication protocol.

OGC Document OGC 10-069r2 [130] describes a layer replication interface service for geospatial databases using WFS and the Atom protocol (RFC 4287 [131] and RFC 5023 [132]). 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, resolution feed, and a replication feed. The SI layer replication interface is patterned after the replication feed described within OGC 10-069r2.

Note: OGC 10-069r2 is an OGC Public Engineering Report, not a standard. OGC 10-069r2 is not believed to be definitive enough to enable multiple interoperable implementations. A future OGC specification or a future revision of this document will describe the protocol definitively.

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

### 5.4.1 Operational Considerations

The SI is not used directly in call processing, although its data is critical to achieving proper routing. For that reason, a single SI system, with frequent backup operations is sufficient.

## 5.5 MSAG Conversion Service (MCS)

The MSAG Conversion Service provides a convenient way to provide data to, or get data from, an un-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 [76] and RFC 5491 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.

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 as described above, plus any layers needed to construct the MSAG for the local jurisdiction. These would typically include an MSAG Community Name, often includes the County ID, and for many jurisdictions where prefix/suffix and/or directionals are included in the Street Name, would include a Street Name layer. Where the content of the MSAG is the same (for all addresses in the jurisdiction) as the equivalent PIDF-LO field, the layer need not be present.

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 where 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.

**PIDFLOtoMSAGRequest**

| Parameter | Condition | Description |
|---|---|---|
| pidflo | Mandatory | PIDF-LO to be converted |

**PIDFLOtoMSAGResponse**

| Parameter | Condition | Description |
|---|---|---|
| msag | Conditional, must be present if conversion succeeds | MSAG resulting from conversion |
| referral | Conditional, must be present if conversion succeeds | URI of another MCS |
| statusCode | Mandatory | Response from operation |

Either msag or referral must be present in the response.

Status Codes

200 Okay No error

512 No Address Found: the input appears to be within the service boundary of the MCS, but no point matching the input was located

515 Unknown MCS/GCS the input is not in the service boundary of the MCS and the local MCS could not locate an MCS who served that location.

504 Unspecified Error

The MSAGtoPIDFLO function works in the same manner, locating the point in the database the MSAG address refers to, and composing a PIDF-LO from the PIDF-LO layers.

**MSAGtoPIDFLORequest**

| Parameter | Condition | Description |
|---|---|---|
| msag | Mandatory | msag to be converted |

**MSAGtoPIDFLOResponse**

| Parameter | Condition | Description |
|---|---|---|
| pidflo | Conditional, must be present if conversion succeeds | PIDF-LO resulting from conversion |
| referral | Conditional, must be present if conversion succeeds | URI of another MCS |

| Parameter | Condition | Description |
|---|---|---|
| statusCode | Mandatory | Response from operation |

Either pidflo or referral must be present in the response.

Status Codes

200 Okay No error (optional to return)

512 No Address Found: the input appears to be within the service boundary of the MCS, but no point matching the input was located

515 Unknown MCS/GCS: the input is not in the service boundary of the MCS and the local MCS could not locate an MCS who served that location.

504 Unspecified Error

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.

### 5.6 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 [76] and RFC 5491 [75], 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 geocode is typically less accurate than geocoding, although some error and unquantified uncertainty is inherent in both.

The Geocode function locates the point in the database represented by the input PIDF-LO and retrieves the geo associated with that location. It constructs a PIDF-LO with the geo. 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.

**GeocodeRequest**

| Parameter | Condition | Description |
|---|---|---|
| pidflo | Mandatory | PIDF-LO with civic to be converted |

**GeocodeResponse**

| Parameter | Condition | Description |
|---|---|---|
| pidflo | Conditional, must be present if conversion succeeds | PIDF-LO resulting from conversion |
| referral | Conditional, must be present if conversion succeeds | URI of another GCS |
| statusCode | Mandatory | Response from operation |

Either pidflo or referral must be present in the response.

Status Codes

200 Okay No error

512 No Address Found: the input appears to be within the service boundary of the GCS, but no point matching the input was located.

515 Unknown MCS/GCS: the input is not in the service boundary of the GCS and the local GCS could not locate a GCS who served that location.

504 Unspecified Error

The ReverseGeocode function works in the same manner, locating the location in the database the input geo refers to, and composing a PIDF-LO from the PIDF-LO layers.

**ReverseGeocodeRequest**

| Parameter | Condition | Description |
|---|---|---|
| pidflo | Mandatory | PIDF-LO with geo to be converted |

**ReverseGeocodeResponse**

| Parameter | Condition | Description |
|---|---|---|
| pidflo | Conditional, must be | PIDF-LO resulting from conversion |

| Parameter | Condition | Description |
|---|---|---|
| | present if conversion succeeds | |
| referral | Conditional, must be present if conversion succeeds | URI of another GCS |
| statusCode | Mandatory | Response from operation |

Either pidflo or referral must be present in the response.

Status Codes

200 Okay No error

512 No Address Found: the input appears to be within the service boundary of the GCS, but no point matching the input was located.

515 Unknown MCS/GCS: the input is not in the service boundary of the GCS and the local GCS could not locate a GCS who served that location.

504 Unspecified Error

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.

Note: The IETF geopriv working group is considering the definition of a geocoding protocol/service. If such a standardization effort is undertaken, and if the resulting work is suitable, it will replace this NENA-only interface in a future revision of this document.

## 5.7 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 other NENA documents. A PSAP provides the following interfaces towards the ESInet.

### 5.7.1 SIP Call interface

The PSAP must deploy the SIP call interface as defined in Section 4.1 including the multimedia capability, and the non-human-initiated 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: field and the absence of the sos service URN in a Request-URI header). The SIP call interface may also be used to place non 9-1-1 calls (including voice-only call backs) from the PSAP using normal SIP Trunking mechanisms as specified in SIPConnect V1.0 [107]. Call backs may be placed to any network that will accept them using the SIP call interface as defined in Section 4.14.1, with the exception that a Geolocation header would not be included, the Request URI would be the URI of the caller, no Route header would be needed and a SIP-Priority header must be included with a parameter value of "psap-callback" [178]. Outgoing calls may be placed via the ESInet using the ESRP as an outgoing proxy server, see Section 5.2.2.1. In most circumstances the ESRP will forward calls through a (configured) BCF to a public network, which might use a User to Network Interface via a public network or a Network to Network Interface via a transit network.

Note: Handling of media other than voice-only callbacks is incompletely specified and will be addressed in a future revision of this document. A new Functional Element that handles call backs, and specifically deals with the requirements for labeling such calls for IMS-based origination networks will be defined in a future revision of this document.

### 5.7.2 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.

### 5.7.3 LoST interface

The PSAP must implement a LoST client interface as defined in Section 4.4. 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:nena: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 direct a call to.

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:nena:service:agencyLocator". The AgencyLocator record can be retrieved from the URI by dereferencing it with HTTPS GET. [5.16.1]What is returned is the Agency Locator record document. From the AgencyLocator record, other interface points, such as a URI to send an EIDD to may be found.

### 5.7.4 LIS Interfaces

The PSAP must implement both SIP Presence Event Package and HELD dereferencing interfaces to any LIS function as described in Section 5.10. When the PSAP receives a location reference (in a

Geolocation header on the upstream SIP interface[34]) 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[35]. The PSAP must use TCP with either TLS or IPsec 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 where used) connections to LISs that it has frequent transactions with. 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 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 [31]. 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 is available. By setting the expiration time of the subscription, the PSAP is able to control what updates it receives. PSAPs that wish to track the motion of a caller could use the location filter and event rate control mechanisms [102] and rate-control [112] to control updates.

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 query” function, also known as “Reverse-ALI” in E9-1-1. ALI has no equivalence in NG9-1-1.

### 5.7.5 Bridge Interface

A PSAP may deploy a bridge (as described in Section 5.8) 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.

### 5.7.6 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 3.4.2.

### 5.7.7 ServiceState

The PSAP must deploy a ServiceState notifier as described in Section 3.4.3.

[34] If the PSAP receives a call via a transfer from another agency, the location of the caller will be found in the EIDD included in the transfer and not in a Geolocation header.

[35] This document specifies that the LIS accept credentials issued to the PSAP traceable to the PCA. Not withstanding that requirement, ESInet elements needing location, including PSAPs, must be able to be provisioned with credentials acceptable to LISs that do not accept the PCA credential.

### 5.7.8 AbandonedCall Event

The PSAP must implement the subscriber side of the AbandonedCall Event as described in Section 5.2.2.9.

### 5.7.9 DequeueRegistration

The PSAP must implement a DequeueRegistration client, as described in Section 5.2.1.4 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 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 the call is destined for.

### 5.7.10 QueueState

The PSAP must implement a QueueState notifier as described in Section 5.2.1.3 for all queues it manages.

### 5.7.11 SI

The PSAP may provide[36] a GIS server interface, as described in Section 4.6 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).

### 5.7.12 Logging Service

The PSAP must implement a Logging Service client as defined in Section 5.13, including the client side of the media recording mechanism (Section 5.13.2). Provisioning controls whether the PSAP records media. The PSAP may deploy a logging service (as described in Section 5.13) 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.

### 5.7.13 Security Posture

The PSAP must provide a Security Posture notifier as described in Section 3.4.1.

### 5.7.14 Policy

The PSAP may provide a Policy Store as described in Section 4.3.1, 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 Termination-Policy in the upstream PRF for the queue(s) its calls are sent to.
PSAPs must also provide an enqueuer policy to specify which entities are allowed to send it calls.

[36] The GIS system may be provided by a 9-1-1 Authority.

### 5.7.15 Additional Data Dereference

The PSAP must deploy a dereference (HTTPS GET) interface for additional data as described in Section 8, as well as the IS-ADR identity query mechanism. PSAP policy may dictate whether Additional Data is retrieved and used. The PSAP must also be able to dereference an EIDD URI for a call transferred to it.

### 5.7.16 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.

### 5.7.17 Test Call

PSAPs must support the test call interface as described in Section 10, 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.

Support for testing of Policy Routing Rules will be addressed in a future issue of this document.

### 5.7.18 Call Diversion

A PSAP may be overloaded and be unable to get every call answered by a call taker. Overload is determined by exceeding the size of the primary queue that its calls are sent to. 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 from. Since the diverted-to PSAP(s) have to explicitly permit (via enqueuePolicy 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.

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”.

### 5.7.19 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 MergeIncident log record and sends an EIDD with a Merge Information component. Incidents can also be linked or split as described in the Logging Service, Section 5.13. The actual IncidentTrackingID would be part of the EIDD 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 ClearIncident record.

## 5.8 Bridging

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 secondary 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. The rough transfer sequence, based on the procedures defined in RFC 4579 [51], 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 (secondary PSAP for example) to the conference
5. PSAP tears down its leg to the conference, the secondary PSAP and the caller remain
6. Secondary PSAP REFERs the caller to it
7. Secondary PSAP terminates the conference.

All Bridges in the ESInet must implement the Session Recording Client interface defined by SIPREC [153]. Provisioning may control whether the bridge does log media.

When the bridge is used to transfer the call, the location of the caller and any Additional Data included with the call must be transferred to the transfer target. 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 EIDD and include it in the transfer operation. The transferor creates the EIDD and includes a Call-Info header field with a purpose parameter of “eidd” as an escaped header field in the Refer-To header. The bridge will then include this header in the INVITE it sends to the transfer target. The EIDD includes the location reported for the caller (in the form it received it, i.e. by-value or by-reference) and any Additional Data included in the call.

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 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.

Note: There are four mechanisms specified for call transfer, due to earlier lack of agreement within the working group. There is a desire to revisit this issue and see if some options can be eliminated.

### 5.8.1 Bridge Call Flow

Conferencing procedures are documented in RFC 4579. 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, and if it were not, its SUBSCRIBE to the conference package would not occur. It is required that the caller, or some element in the path, implement the Replaces header, see Section 5.9.

#### 5.8.1.1 Creation of a Conference Using SIP Ad-Hoc Methods

This scenario described in the call flow depicted below follows Section 5.4 of RFC 4579.

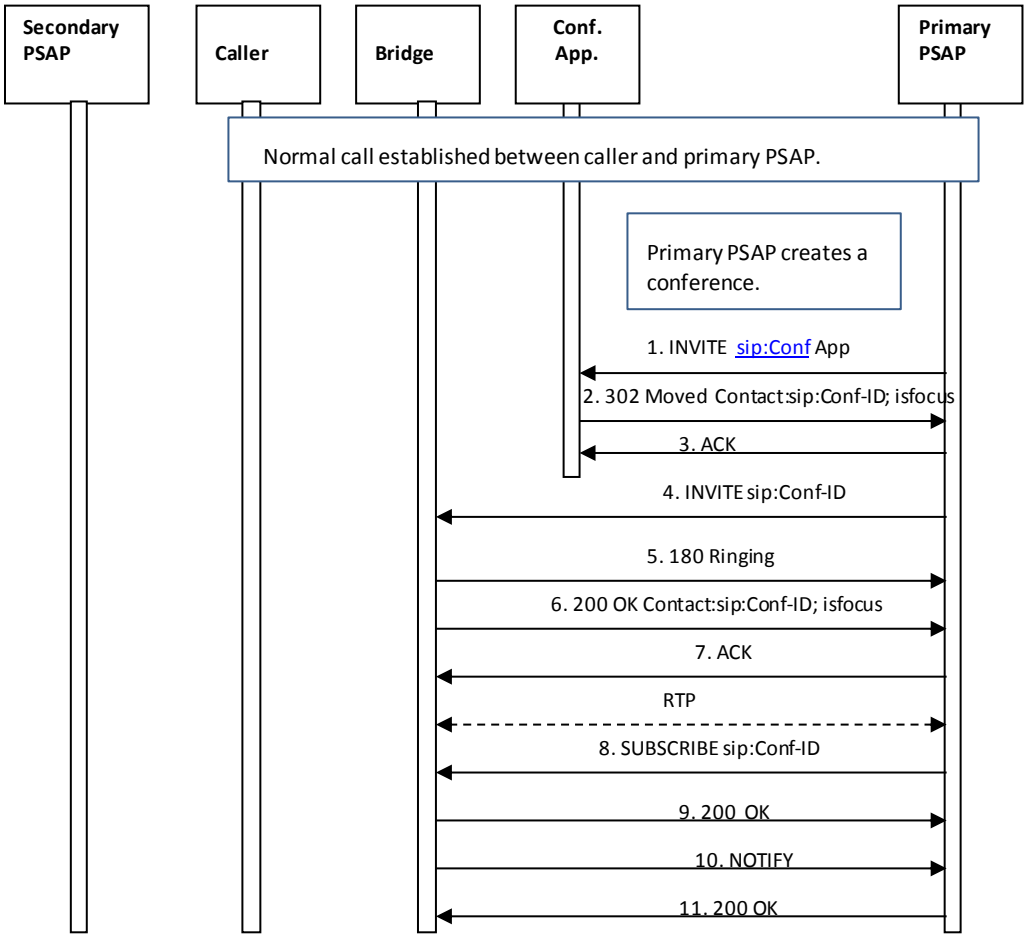



**Figure 5-1 Ad-Hoc Conference Call Flow Using SIP**

1. The Primary PSAP creates a conference by first sending an INVITE to a conference application, using a URI that is known by/provisioned at the Primary PSAP.

2. The Conference Application responds by sending a 302 Moved message, which redirects the Primary PSAP to the conference bridge, and provides the Conference-ID that should be used for the conference.
3. The Primary PSAP acknowledges the receipt of the 302 Moved message.
4. The Primary PSAP generates an INVITE to establish a session with the conference bridge[37].
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 Primary PSAP and the conference bridge.
7. The Primary PSAP returns an ACK message in response to the 200 OK.
8. through 11. Once the media session is established, the Primary PSAP subscribes to the conference associated with the URI obtained from the Contact header provided in the 200 OK message from the conference bridge.

#### 5.8.1.2 Primary PSAP Asks Bridge to Invite the Caller to the Conference

This flow is based on Section 5.10 of RFC 4579 [51].

[37] 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.

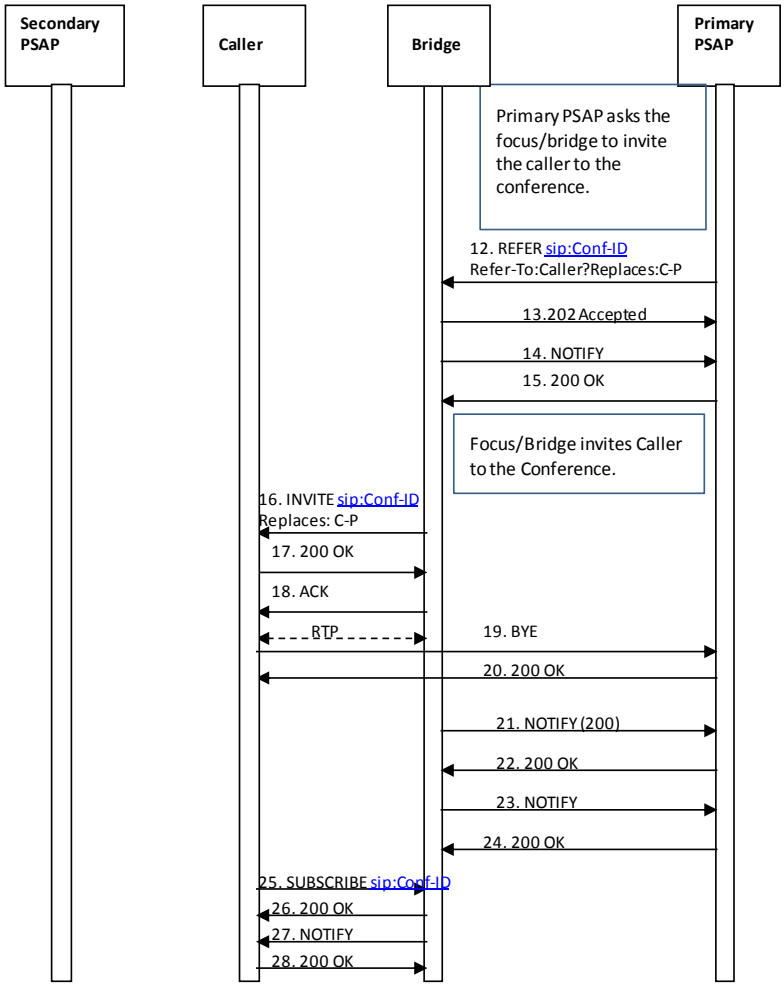



**Figure 5-2 Primary PSAP Asks Bridge to Invite the Caller to the Conference**

12. After the Primary PSAP establishes the conference, it sends a REFER method to the conference bridge asking it to invite the caller to the conference. The REFER method contains an escaped Replaces header field in the URI included in the Refer-To header field.
13. The bridge returns a 202 Accepted message to the Primary PSAP.
14. The bridge then returns a NOTIFY message, indicating the subscription state of the REFER request (i.e., active).
15. The Primary 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 Conf-ID and a Replaces header that references the leg between the caller and the Primary PSAP.
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.*

19. The caller releases the connection to the Primary PSAP by sending a BYE message.
20. The Primary PSAP responds by returning a 200 OK message.
21. The bridge sends a NOTIFY message to the Primary PSAP to provide REFER processing status.
22. The Primary PSAP responds by returning a 200 OK message.
23. The bridge sends a NOTIFY message to the Primary PSAP to provide updated status associated with the conference state.
24. The Primary PSAP responds by returning a 200 OK message.
25. The caller subscribes to the conference associated with the Conference ID 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)

#### 5.8.1.3 Secondary PSAP is Invited to the Conference

This flow is based on Section 5.5 of RFC 4579.

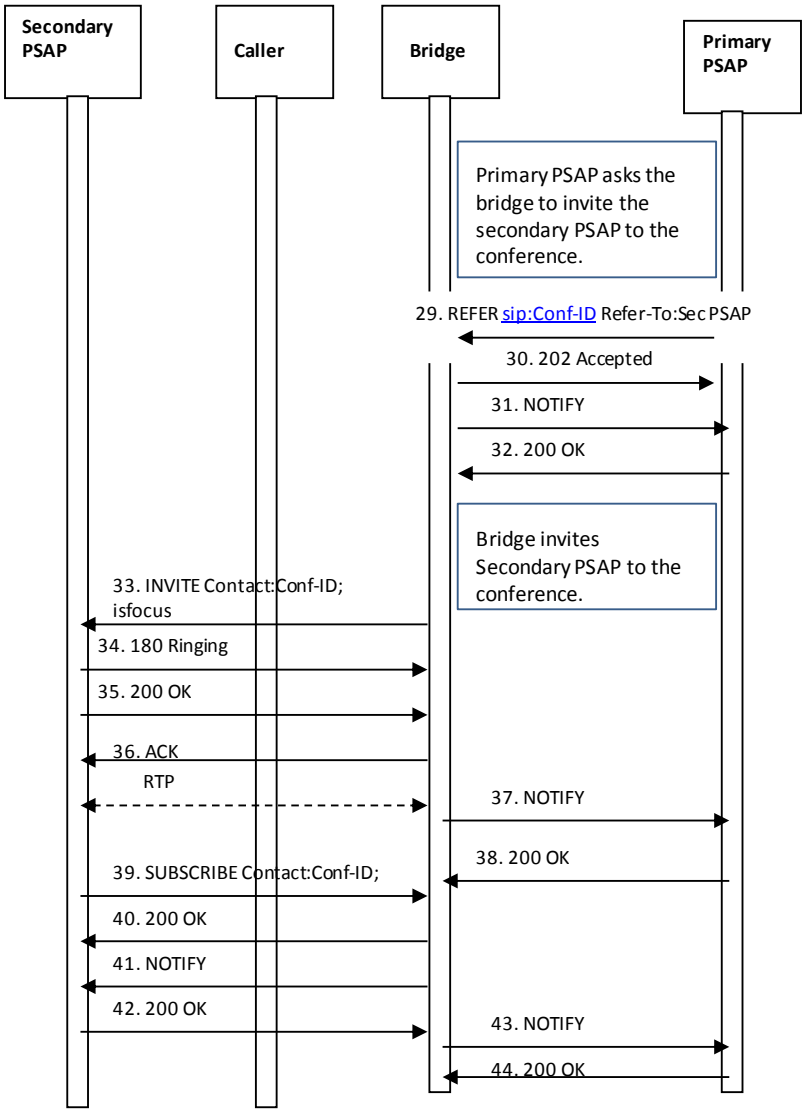



**Figure 5-3 Secondary PSAP Invited to Conference**

29. The Primary PSAP sends a REFER method to the conference bridge asking it to invite the Secondary PSAP to the conference. The REFER method contains the Conf-ID and a Refer-To header that contains the URI of the Secondary PSAP. The REFER method also contains an escaped Call-Info header field containing a reference URI that points to the EIDD data structure and a purpose parameter of "eidd".
30. The bridge returns a 202 Accepted message to the Primary PSAP.
31. The bridge then returns a NOTIFY message, indicating that subscription state of the REFER request (i.e., active).
32. The Primary PSAP returns a 200 OK in response to the NOTIFY message.
33. The bridge invites the Secondary PSAP to the conference by sending an INVITE method containing the Conf-ID and Contact header 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 EIDD data structure and a purpose parameter of "eidd".

34. The Secondary PSAP UA responds by returning a 180 Ringing message to the bridge.
35. The Secondary 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 Secondary PSAP and the bridge.*

37. The bridge returns a NOTIFY message to the Primary PSAP to provide updated status of the subscription associated with the REFER request.
38. The Primary PSAP responds to the NOTIFY message by returning a 200 OK message.
39. The Secondary PSAP subscribes to the conference associated with the Conf-ID 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 Secondary PSAP.
41. The bridge then returns a NOTIFY message to the Secondary PSAP to provide subscription status information.
42. The Secondary PSAP responds by returning a 200 OK message.
43. The bridge sends a NOTIFY message to the Primary PSAP providing updated status for the subscription associated with the REFER request.
44. The Primary PSAP responds to the NOTIFY message by returning a 200 OK message.

*At this point the caller, Primary PSAP, and Secondary PSAP are all participants in the conference.*

#### 5.8.1.4 Primary PSAP Drops Out of Conference; Secondary PSAP Completes Transfer

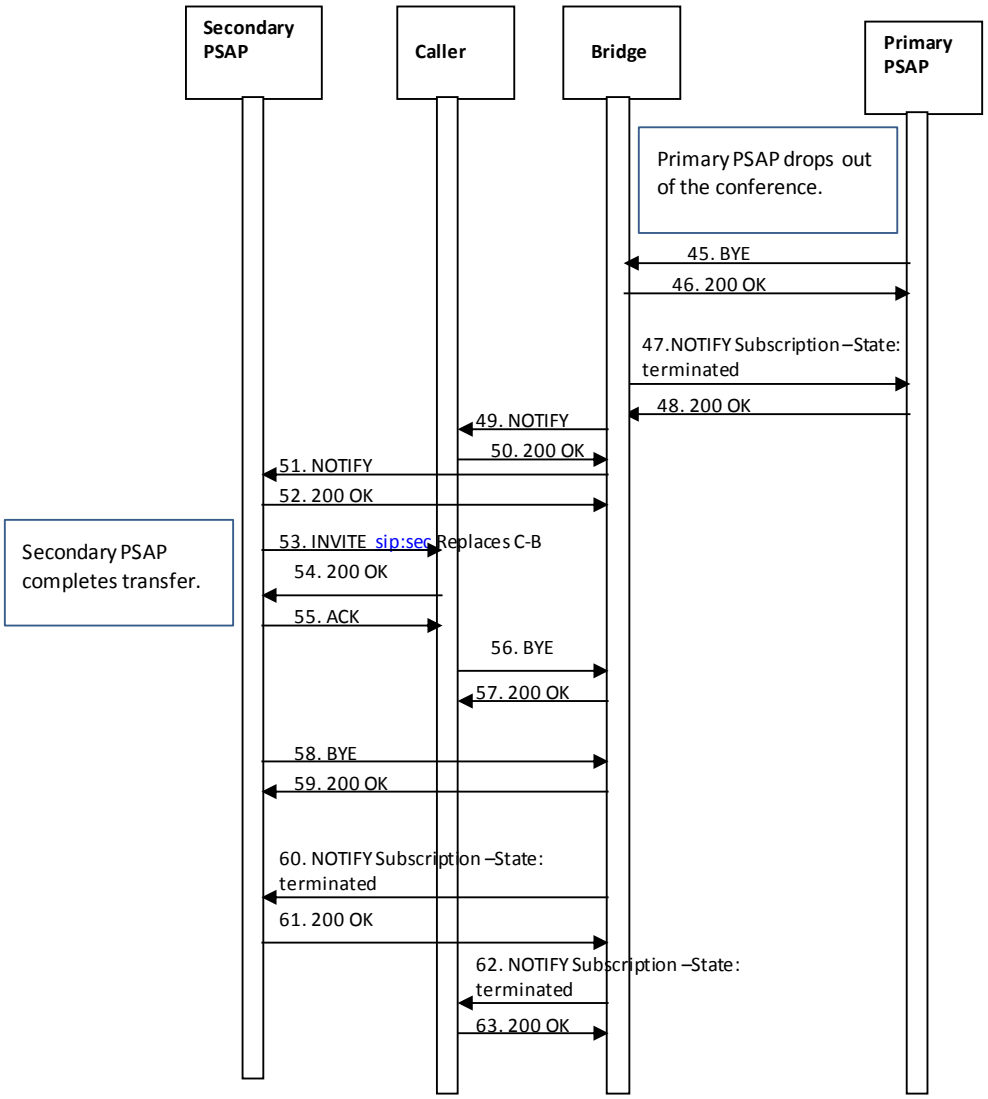



**Figure 5-4 Primary PSAP Drops, Secondary Completes Transfer**

45. Upon determining that the emergency call transfer should be completed, the Primary PSAP disconnects from the call by sending a BYE message to the bridge.
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 Primary 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 Secondary PSAP indicating that there has been a change to the subscription state.
52. The Secondary PSAP returns a 200 OK in response to the NOTIFY.

53. Upon recognizing that the caller and the Secondary PSAP are the only remaining participants in the conference, the Secondary 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 secondary PSAP. The secondary 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 Secondary PSAP.
55. The Secondary PSAP returns an ACK in response to the 200 OK.
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 Secondary 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 Secondary PSAP.
60. The bridge then returns a NOTIFY message to the Secondary PSAP indicating that the subscription to the conference has been terminated.
61. The Secondary 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 Secondary PSAP are involved in a two-way call.*

### 5.8.2 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 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 Document (EIDD) structure (See Section 8 for further discussion of Additional Data structures). When an emergency call is transferred, the transferring PSAP will request that the bridge inserts by embedded header, a Call-Info header field with a URI that points to the EIDD data structure in the REFER method sent to the bridge, and a purpose parameter of "eidd". The bridge must subsequently include this Call-Info header field in the INVITE it sends to the transfer target.

When transferring a 9-1-1 call, the transferring PSAP must supply an EIDD containing the information that represents the current state of the incident/call. The EIDD is passed in an escaped Call-Info header field with a purpose of "eidd" that is within the Refer-To header. The EIDD must be passed by reference, where the Call-Info header field contains a URL that when dereferenced yields the EIDD. While the EIDD 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 EIDD in a mime type of xml+nena/eidd), such a construct could not be invoked at the bridge by an embedded header in the Refer-To: from the transferring PSAP. To dereference the

URI and obtain the EIDD, the recipient does an HTTPS: GET on the URI and the EIDD [188] is returned.

The EIDD contains a snapshot of the state of the Incident, as known by the sending Agency. Obtaining updates to Incident state will be defined in a future version of this document.

## 5.9 Transfer Involving Calling Devices that Do Not Support Replaces

As discussed in Section 5.7 of NENA 08-002 [100], there is a problem that some devices that could originate 9-1-1 calls do not support the Replaces header. 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. Section 5.7 of NENA 08-002 describes three solutions to this problem. Each of these solutions is specified in more detail in the sections below.

Note: There are four mechanisms specified for call transfer, due to earlier lack of agreement within the working group. There is a desire to revisit this issue and see if some options can be eliminated.

### 5.9.1 B2BUA

When this solution is implemented, some element in the initial call path from the BCF to the first PSAP that answers the call must include a B2BUA function as described in RFC 3261 [12]. All calls are relayed through the B2BUA. The B2BUA is transparent to signaling with the following exceptions:

1. Media endpoints towards both the caller and the PSAP are rewritten to be contained within the B2BUA.
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 containing the replaces option-tag it must include a Supported header containing the replaces option-tag in the INVITE forwarded to the ESInet and provide the functionality described in this section.

Note that the following flow assumes that the Primary PSAP has already created a conference using SIP Ad Hoc methods, as described in Section 5.7.1.1 of NENA 08-002.

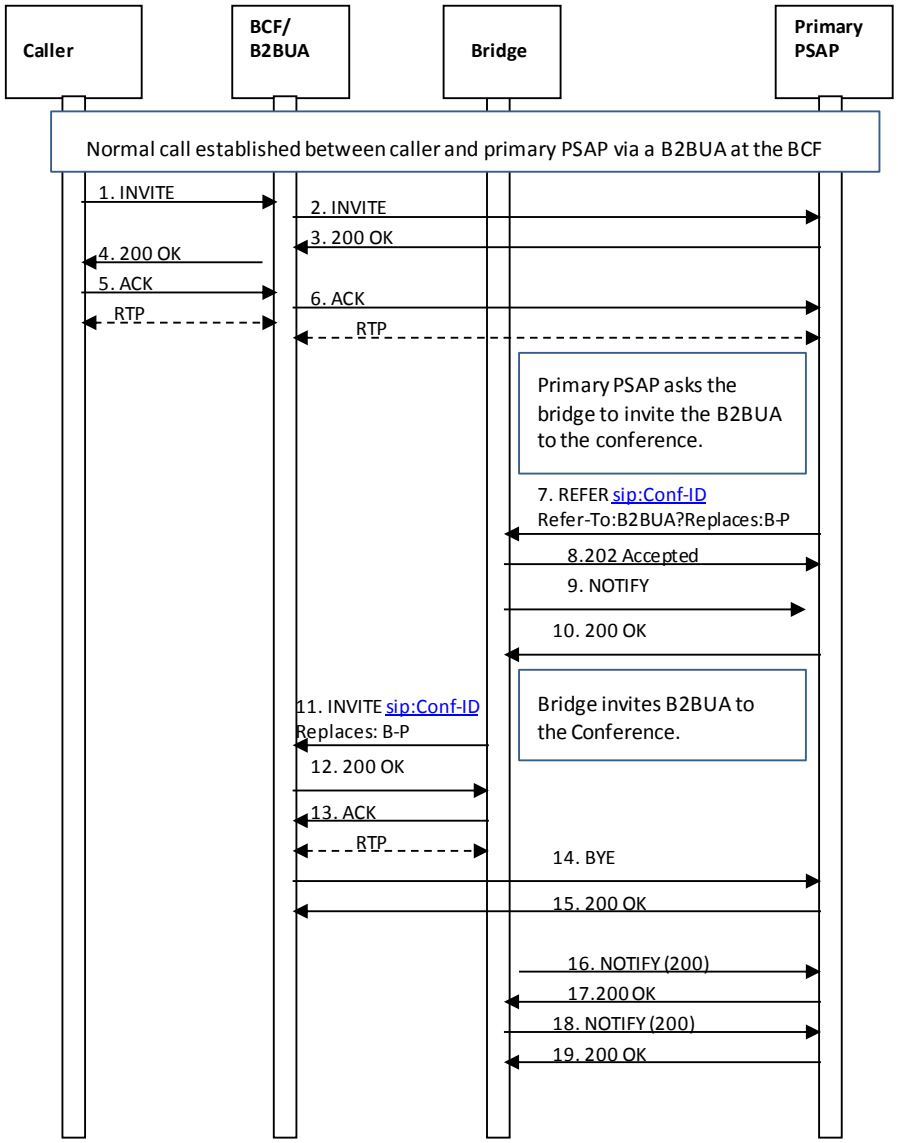



**Figure 5-5 Call Transfer Involving a B2BUA**

1. The caller initiates an emergency session request by sending an INVITE message to the B2BUA. The INVITE contains a Geolocation header with caller location information.
2. The B2BUA sends a corresponding INVITE message via the i3 ESInet toward the Primary PSAP. (Elements and signaling involved in routing the emergency call within the i3 ESInet are not shown in this flow). The INVITE would contain a Supported header indicating support for Replaces.
3. The Primary PSAP responds by returning a 200 OK message to the B2BUA.
4. The B2BUA responds to the receipt of the 200 OK from the Primary PSAP by sending a 200 OK message to the caller's device.
5. The caller's device responds by sending an ACK to the B2BUA.

*A media session is established between the caller and the B2BUA. Depending on the design of the ESInet, the B2BUA may cross connect media from the caller to the Primary PSAP*

6. The B2BUA sends an ACK to the Primary PSAP in response to receiving an ACK from the caller's device.

   *A media session is established between the B2BUA and the Primary PSAP.*

7. The Primary PSAP sends a REFER method to the conference bridge asking it to invite the B2BUA to the conference. The REFER method contains an escaped Replaces header field in the URI included in the Refer-To header field.
8. The bridge returns a 202 Accepted message to the Primary PSAP.
9. The bridge then returns a NOTIFY message, indicating that subscription state of the REFER request (i.e., active).
10. The Primary PSAP returns a 200 OK in response to the NOTIFY message.
11. The bridge invites the B2BUA to the conference by sending an INVITE method containing the Conf-ID and a Replaces header that references the leg between the B2BUA and the Primary PSAP.
12. The B2BUA accepts the invitation by returning a 200 OK message.
13. The bridge acknowledges receipt of the 200 OK message by returning an ACK.

    *A media session is established between the B2BUA and the bridge. Note that the media session between the B2BUA and the Primary PSAP still exists at this time. Note also that the media session between the caller and the B2BUA is undisturbed. As above, the B2BUA may cross connect media from the caller to the bridge*

14. The B2BUA releases the connection to the Primary PSAP by sending a BYE message.
15. The Primary PSAP responds by returning a 200 OK message.

    *At this point, the media session between the B2BUA and the Primary PSAP is torn down.*

16. The bridge sends a NOTIFY message to the Primary PSAP to provide updated status of the subscription associated with the REFER request.
17. The Primary PSAP responds by returning a 200 OK message.
18. The bridge sends a NOTIFY message to the Primary PSAP to provide updated status of the subscription associated with the REFER request.
19. The Primary PSAP responds by returning a 200 OK message.

At this point, the Primary PSAP requests that the bridge add the Secondary PSAP to the conference, following the flow described in Section 5.8.1.3. Once the Primary PSAP determines that the transfer can be completed, it drops off the call, following the flow described in Section 5.8.1.4. The Secondary PSAP then completes the transfer as illustrated below. Note that the connection between the caller and the B2BUA is unaffected by the Primary PSAP disconnecting or the completion of the transfer by the Secondary PSAP. The following flow also illustrates termination of the emergency call initiated by the Secondary PSAP.

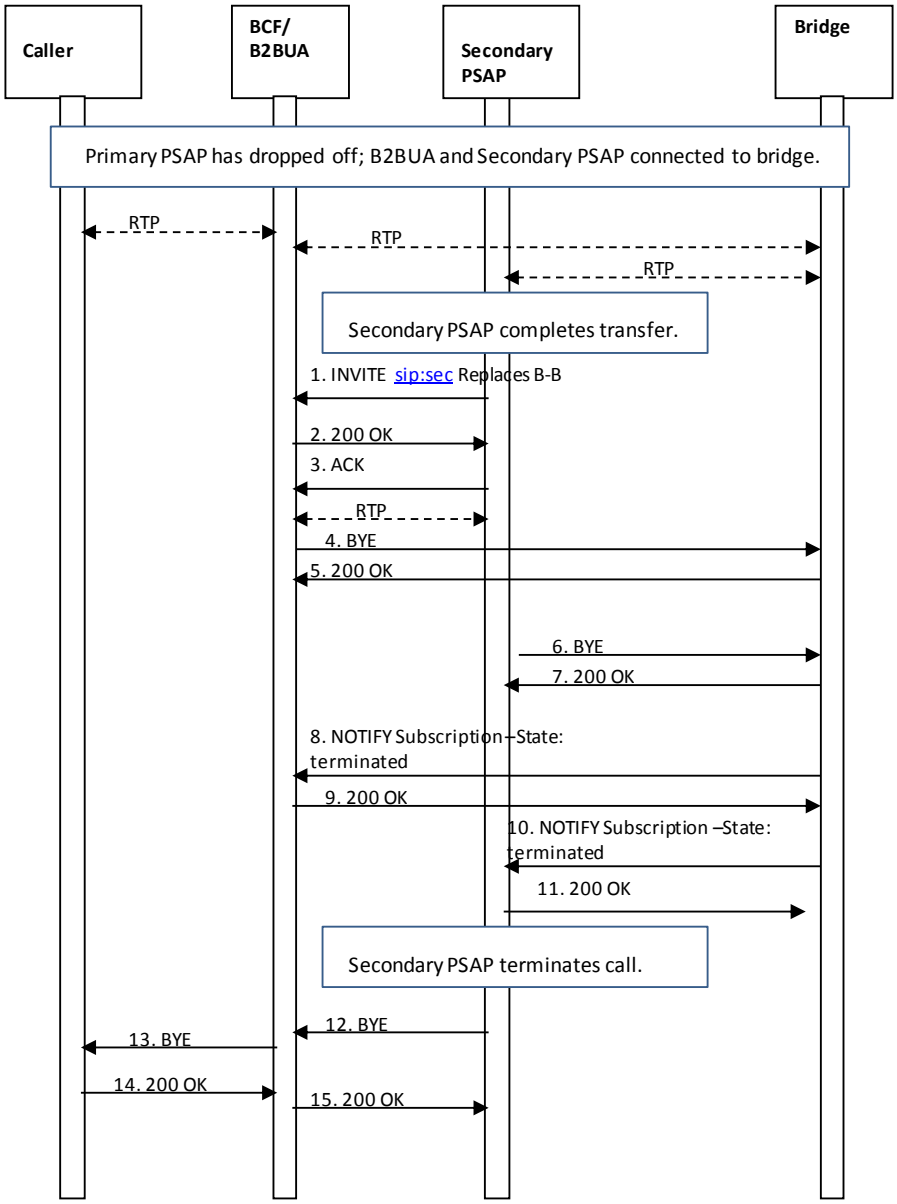



**Figure 5-6 Primary PSAP Drops, Secondary Completes Transfer**

1. The Secondary PSAP completes the transfer by sending an INVITE to the B2BUA requesting that it replaces its connection to the bridge with a direct connection to the Secondary PSAP. The Secondary PSAP learns the URI of the B2BUA from the entity attribute in the endpoint section of the user's container in the conference NOTIFY from the bridge.
2. The B2BUA responds by returning a 200 OK message to the Secondary PSAP.
3. The Secondary PSAP returns an ACK in response to the 200 OK.

*At this point, a media session is established between the B2BUA and the Secondary PSAP. The media session between the B2BUA and the bridge also still exists at this time. The B2BUA may cross connect media as per above*

4. The B2BUA then sends a BYE to the bridge to terminate the session.
5. The bridge responds by sending the B2BUA a 200 OK message.

   *At this time the media session between the B2BUA and the bridge is torn down.*

6. The Secondary PSAP also terminates its session with the bridge by sending a BYE message to the bridge.
7. The bridge responds by sending a 200 OK message to the Secondary PSAP.

   *At this point, the media session between the Secondary PSAP and the bridge is torn down.*

8. The bridge then returns a NOTIFY message to the B2BUA indicating that the subscription to the conference has been terminated.
9. The B2BUA responds with a 200 OK message.
10. The bridge then returns a NOTIFY message to the Secondary PSAP indicating that the subscription to the conference has been terminated.
11. The Secondary PSAP responds with a 200 OK message.

    *At this point, the transfer is complete, and the caller and the Secondary PSAP are involved in a two-way call.*

12. The Secondary PSAP determines that the call should be terminated and sends a BYE message to the B2BUA.
13. The B2BUA sends a BYE message to the caller to terminate the session.
14. The caller sends a 200 OK message to the B2BUA in response to the BYE.
15. The B2BUA sends a 200 OK to the Secondary PSAP in response to receiving the 200 OK from the caller. At this point the emergency session is terminated.

The B2BUA may act as a media relay for all media. All media packets on all negotiated media streams are relayed from one side of the B2BUA to the other.

Characteristics of this solution are:

- The solution is deployed at the edge of the ESInet; the rest of the ESInet can assume Replaces works.
- Media is anchored at the BCF regardless of what happens to the call.
- The B2BUA is call stateful.
- The B2BUA is in the path regardless of whether the device implements Replaces or not.

### 5.9.2 Bridging at the PSAP Using Third Party Call Control in the Call Taker User Agent

RFC 3725 [35] describes a technique in which the initial answering UAC becomes a signaling B2BUA. If this method is chosen in an ESInet, a call taker UA receiving a call which does not contain a Supported header indicating support for Replaces must take the actions described in this section. Unlike the examples in RFC 3725, the caller has a call established with the call taker (which takes on the role of the "controller" in RFC 3725). The call sequence (based on RFC 3725 Flow IV) is described in the following subsections.

### 5.9.2.1 Call Taker Creates a Conference

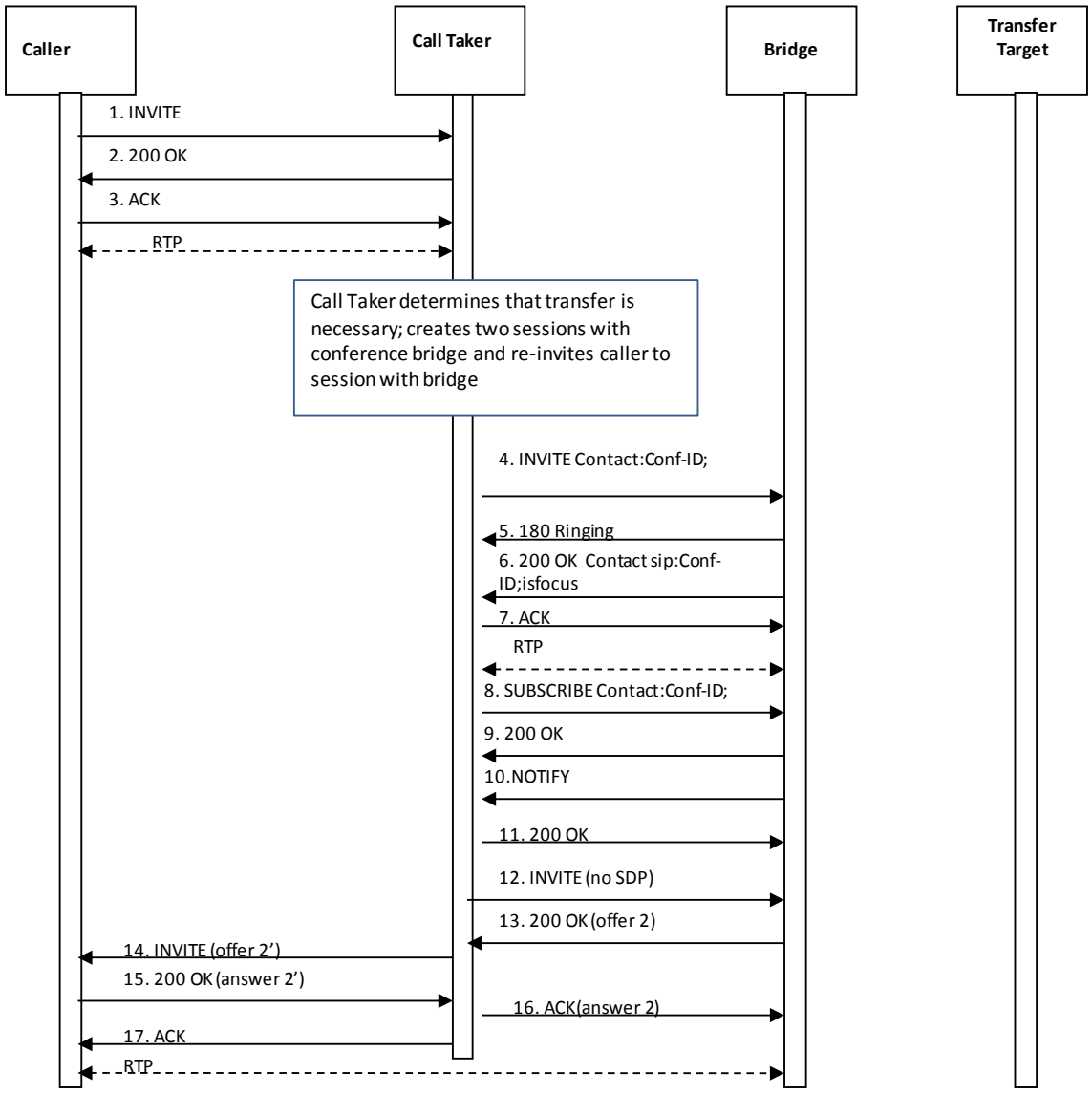



**Figure 5-7 Call Taker Creates Conference**

1. The caller initiates an emergency session request by sending an INVITE message via the i3 ESInet to the Primary PSAP call taker. The INVITE contains a Geolocation header with caller location information (Elements and signaling involved in routing the emergency call within the i3 ESInet are not shown in this flow).
2. The Primary PSAP responds by returning a 200 OK message to the caller's device.
3. The caller's device responds by sending an ACK to the Primary PSAP.

*A media session is established between the caller and the Primary PSAP. The Primary PSAP determines that a transfer is necessary and uses SIP signaling to create a conference with a conference bridge, having previously received a Conference ID from a conference application (as described in Section 5.8.1.1).*

4. The Primary PSAP initiates its first session with the bridge (with media) by sending it an INVITE message containing the Conf-ID**.**
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 Primary PSAP and the conference bridge.
7. The Primary PSAP returns an ACK message in response to the 200 OK.
8. The Primary PSAP subscribes to the conference associated with the Conf-ID by sending a SUBSCRIBE message to the bridge.
9. The bridge responds by returning a 200 OK message.
10. The bridge then sends a NOTIFY message to the Primary PSAP providing the status of the subscription.
11. The Primary PSAP responds to the NOTIFY by returning 200 OK message to the bridge.
12. The Primary PSAP initiates its second session with the bridge (without media) by sending it an INVITE message with no SDP.
13. The bridge responds with a 200 OK that contains an offer (i.e., "offer 2").
14. The Primary PSAP sends a re-INVITE to the caller's device with the new offer.
15. The caller's device responds by sending a 200 OK (providing an answer to the offer) to the Primary PSAP.
16. The Primary PSAP conveys the answer in an ACK sent to the bridge.
17. The Primary PSAP also sends an ACK to the caller's device.

*At this time, a media session is established directly between the caller and the bridge.*

### 5.9.2.2 Call Taker Asks the Bridge to Invite the Transfer Target to the Conference

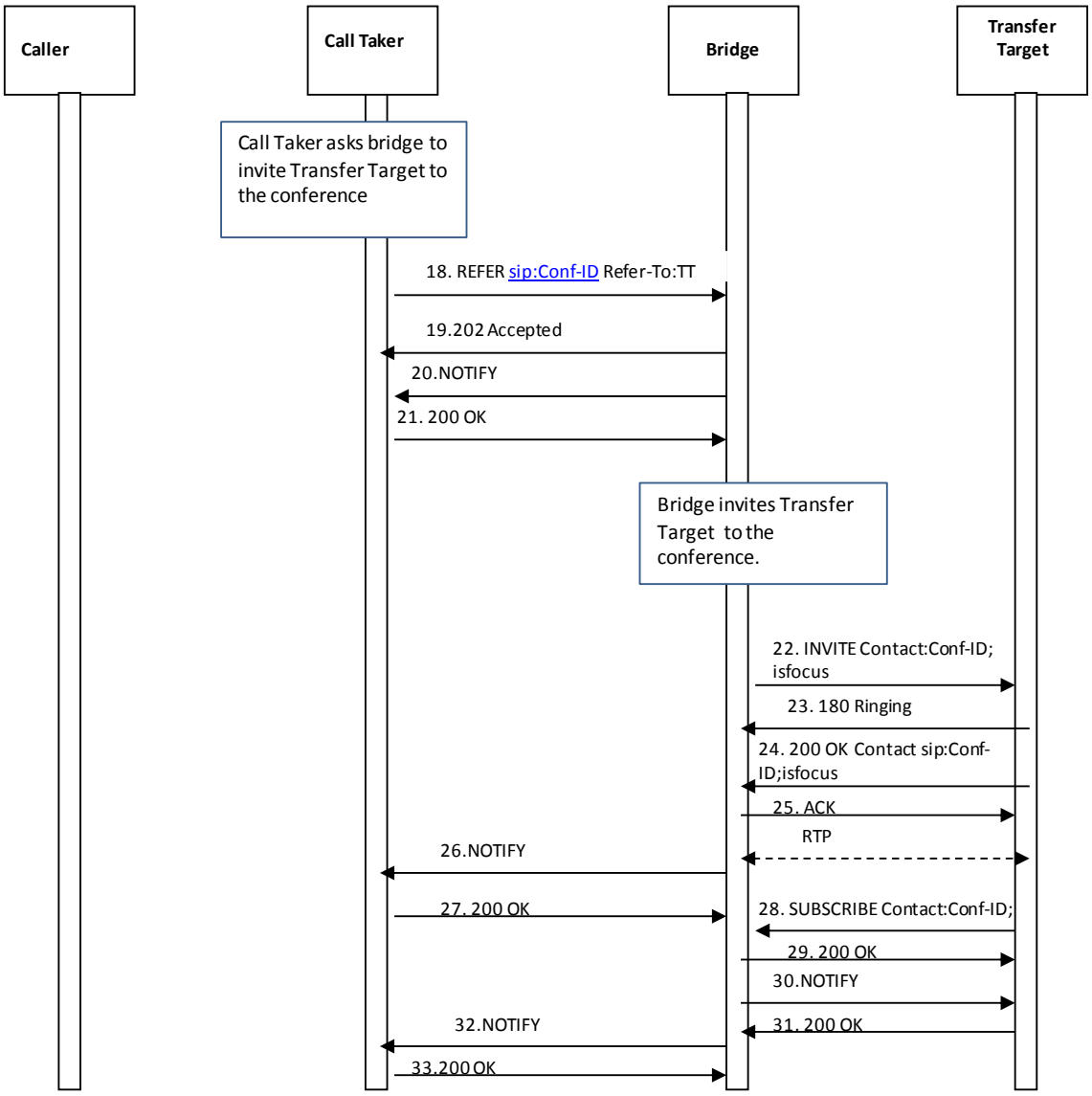



**Figure 5-8 Transfer Target Invited to Conference**

18. The Primary PSAP sends a REFER method to the conference bridge asking it to invite the Transfer Target (i.e., Secondary PSAP) to the conference. The REFER method contains the Conf-ID and a Refer-To header that contains the URI of the Transfer Target. The REFER method also contains an escaped Call-Info header field containing a reference URI that points to an EIDD data structure and a purpose parameter of "eidd".
19. The bridge returns a 202 Accepted message to the Primary PSAP.
20. The bridge then returns a NOTIFY message to the Primary PSAP, indicating that subscription state of the REFER request (i.e., active).
21. The Primary PSAP responds by returning a 200 OK message.

22. The bridge invites the Transfer Target to the conference by sending an INVITE method containing the Conf-ID and the 'isfocus' feature parameter. The INVITE will also have the Call-Info header field containing a reference URI that points to the EIDD data structure and a purpose parameter of "eidd".
23. The Transfer Target responds by returning a 180 Ringing message to the bridge.
24. The Transfer Target accepts the invitation by returning a 200 OK message.
25. The bridge acknowledges receipt of the 200 OK message by returning an ACK.

    *A media session is established between the Transfer Target and the bridge.*
26. The bridge returns a NOTIFY message to the Primary PSAP to provide updated status of the subscription associated with the REFER request.
27. The Primary PSAP responds to the NOTIFY message by returning a 200 OK message.
28. The Transfer Target subscribes to the conference associated with the Conf-ID provided in the INVITE message from the bridge by sending a SUBSCRIBE message to the bridge.
29. The bridge acknowledges the subscription request by sending a 200 OK message back to the Transfer Target.
30. The bridge then returns a NOTIFY message to the Transfer Target to provide subscription status information.
31. The Transfer Target responds by returning a 200 OK message.
32. The bridge sends a NOTIFY message to the Primary PSAP providing updated status for the subscription associated with the REFER request.
33. The Primary PSAP responds to the NOTIFY message by returning a 200 OK message.

    *At this point the caller, Primary PSAP, and Transfer Target are all participants in the conference.*

### 5.9.2.3 Primary PSAP Drops; Transfer Target Completes Transfer

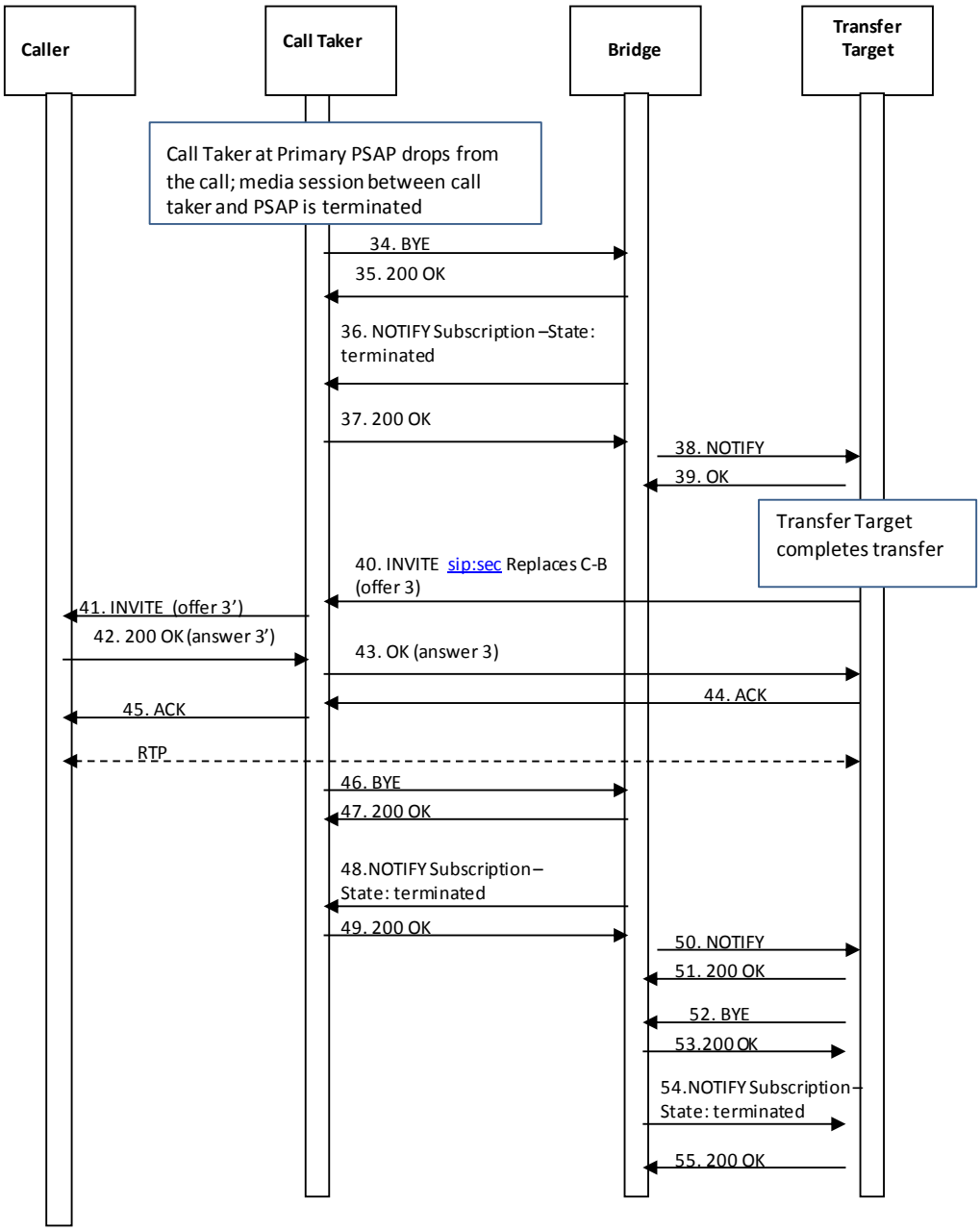



**Figure 5-9 Primary PSAP Drops, Target Completes Transfer**

34. The Primary PSAP initiates termination of its media session with the bridge by sending the bridge a BYE message.
35. The bridge responds by sending the Primary PSAP a 200 OK message.

    *At this time the media session between the Primary PSAP and the bridge is torn down.*

36. The bridge sends a NOTIFY message to the Primary PSAP indicating that the subscription has been terminated.

37. The Primary PSAP responds by returning a 200 OK message.
38. The bridge sends a NOTIFY message to the Transfer Target to provide it updated status information.
39. The Transfer Target replies by returning a 200 OK message.
40. The Transfer Target completes the transfer by sending an INVITE to the Primary PSAP (acting as the B2BUA for the caller) asking it to replace its connection to the bridge (i.e., the media session between the caller and the bridge) with a direct connection to the Transfer Target (with offer 3). Note that the Transfer Target must be aware that it is the Primary PSAP that receives the INVITE.
41. The Primary PSAP sends a re-INVITE to the caller's device asking it to move the media from the bridge to the Transfer Target (with offer 3)
42. The caller's device responds by sending a 200 OK message back to the Primary PSAP (with answer 3).
43. The Primary PSAP sends a 200 OK message to the Transfer Target (with answer 3).
44. The Transfer Target acknowledges the 200 OK message by returning an ACK to the Primary PSAP.
45. The Primary PSAP acknowledges the 200 OK message by returning an ACK to the caller's device.

*At this point, a media session is established directly between the caller and the Transfer Target.*

46. The Primary PSAP sends a BYE to the bridge to terminate the session with the bridge.
47. The bridge responds by sending a 200 OK message to the Primary PSAP.

*At this time the media session between the caller and the bridge is terminated.*

48. The bridge sends the Primary PSAP a NOTIFY message indicating that the subscription has been terminated.
49. The Primary PSAP responds by sending a 200 OK message.
50. The bridge sends the Transfer Target a NOTIFY message to provide it updated information on the status of the conference.
51. The Transfer Target responds by returning a 200 OK message.
52. The Transfer Target sends a BYE to the bridge to terminate the session with the bridge.
53. The bridge responds by sending a 200 OK message to the Transfer Target.

*At this point, the media session between the Transfer Target and the bridge is terminated.*

54. The bridge sends the Transfer Target a NOTIFY message indicating that its subscription has been terminated.
55. The Transfer Target responds by sending a 200 OK message.

#### 5.9.2.4 Transfer Target Terminates Session with Caller

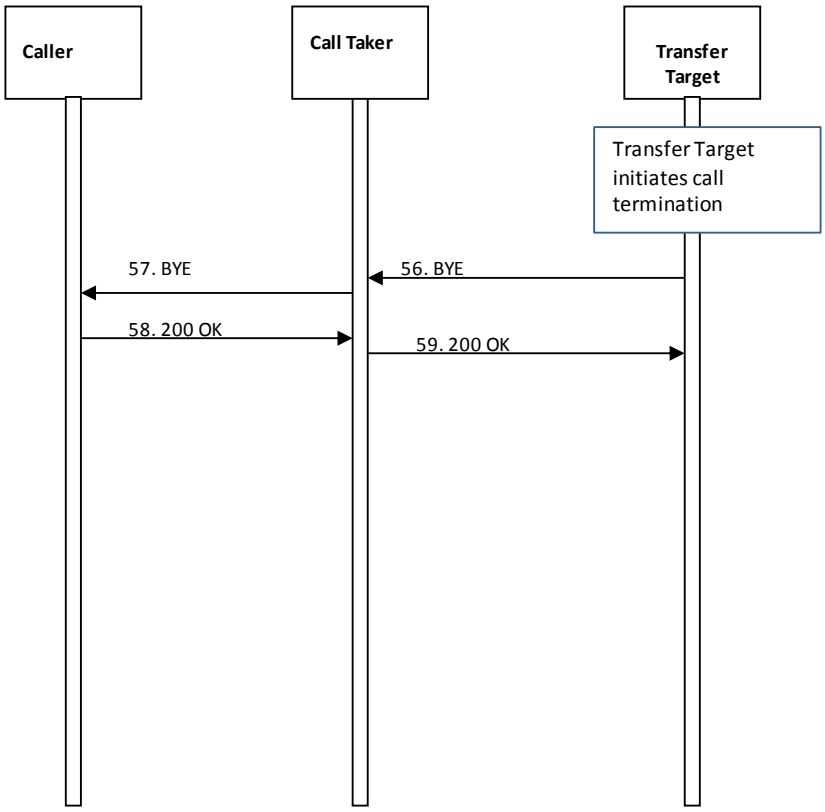



**Figure 5-10 Transfer Target Terminates Call**

56. The Transfer Target initiates call termination by sending the Primary PSAP a BYE message.
57. The Primary PSAP sends a BYE message to the caller's device to initiate request termination of the session.
58. The caller's device responds by returning a 200 OK message to the Primary PSAP.
59. The Primary PSAP responds by returning a 200 OK message to the Transfer Target.

*At this time the media session between the caller and the Transfer Target is terminated.*

In this transfer scenario, the Call Taker UA remains in the signaling path for the duration of the call. The media flows directly (via any BCF firewall of course) between the caller and the Transfer Target. Any further transfers would be accomplished in a similar manner, with the Call Taker UA accepting an INVITE with a Replaces header, and initiating a re-INVITE towards the caller to establish the correct media path.

This sequence is only necessary when the device does not implement Replaces. The Call Taker UA can notice the presence of the Supported header, and if Replaces is supported, it can just initiate a transfer using standard SIP methods, as described in Section 5.7.1. It could, optionally, attempt the Replaces even if a Supported header was not found, detect an error and initiate the re-INVITE as above in response.

The characteristics of this solution are:

- No additional network signaling elements in the path unless necessary

- Media goes direct between endpoints
- Caller UA receives multiple Re-INVITE messages

### 5.9.3 Answer all calls at a bridge

All incoming 9-1-1 calls are answered at a bridge. When the bridge receives a call for the URI specified in the last hop LoST route, the bridge creates the caller to bridge leg, and initiates an INVITE to the PSAP/Call Taker (depending on configuration and where the bridge is located: in the network or in the PSAP). The caller remains on the bridge where it was first answered. 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.

#### 5.9.3.1 Call Established Between Caller and Primary PSAP Via Bridge

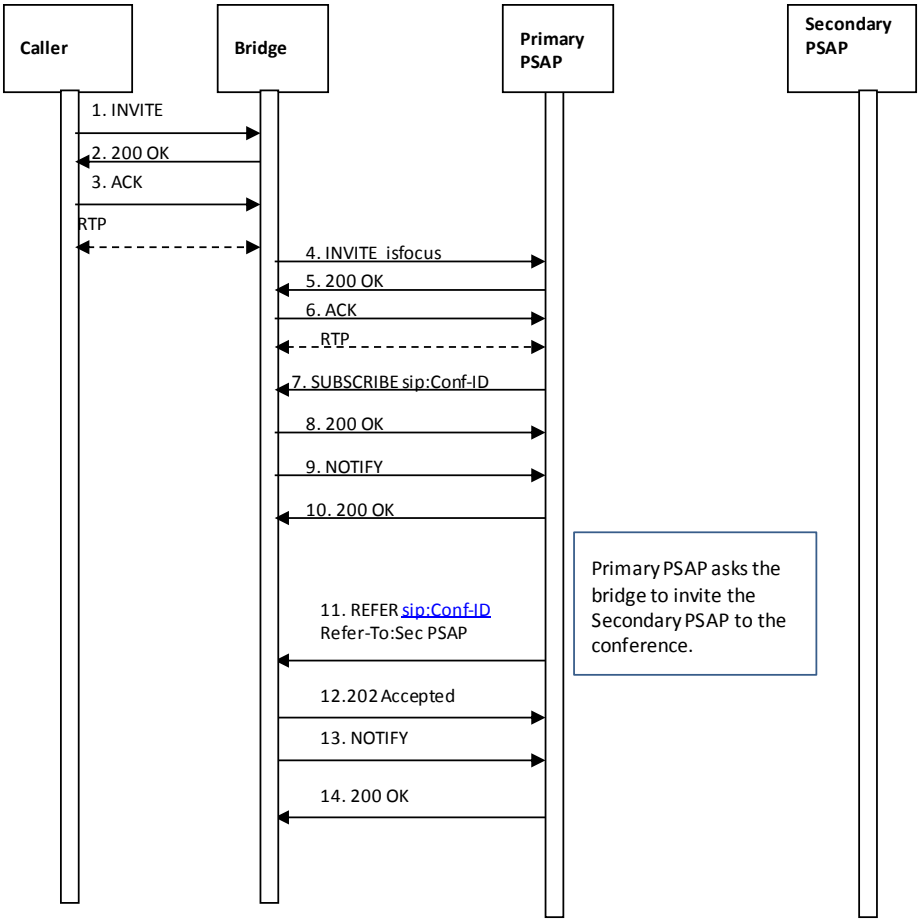



**Figure 5-11 Call Established at Bridge**

1. The caller initiates an emergency session request by sending an INVITE message into the i3 ESInet. The INVITE contains a Geolocation header with caller location information. (Elements and signaling involved in routing the emergency call within the i3 ESInet are not shown in this

flow.) The call is routed using i3 mechanisms, and the URI of the target Primary PSAP is determined. The call is delivered to a bridge in the i3 ESInet.

2. Upon receiving the INVITE from the caller, the bridge responds by returning a 200 OK to the caller.
3. The caller returns an ACK in response to the 200 OK from the bridge.

*A media session is established between the caller and the bridge.*

4. Upon receiving the call at the bridge, the bridge initiates a call to the Primary PSAP by sending an INVITE message. The INVITE must have a RequestURI of "urn:service:sos" and a Route header containing a URI of the PSAP. The INVITE message generated by the bridge should include a Call-Info header field with a purpose parameter of "eidd", with a URI (either an external HTTPS: URI or Content Identifier with a cid: URI) pointing to an EIDD that contains the location of the caller[38], and may contain a Geolocation header with the location of the caller, for backwards compatibility. Any Call-Info header fields that were received in the incoming INVITE message should be in the eidd and may be in the INVITE for backwards compatibility. The identity of the original caller should be in the eidd, and should be in a P-Asserted-Identity (P-A-I) header if a P-A-I was in the original INVITE from the caller.
5. The Primary PSAP responds by returning a 200 OK message to the bridge.
6. The bridge responds by sending an ACK to the Primary PSAP.

*A media session is established between the bridge and the Primary PSAP.*

7. Once the media session is established, the Primary PSAP sends a SUBSCRIBE message to the bridge to subscribe to the conference associated with the Conf-ID identified when the conference was initially established with the bridge.
8. The bridge responds to the SUBSCRIBE message by returning a 200 OK message to the Primary PSAP.
9. The bridge then returns a NOTIFY message to the Primary PSAP to provide it with status information regarding the conference.
10. The Primary PSAP responds to the NOTIFY message by returning a 200 OK message.
11. The Primary PSAP sends a REFER method to the bridge asking it to invite the Secondary PSAP to the conference. The REFER method contains the Conf-ID and a Refer-To header that contains the URI of the Secondary PSAP. The REFER method also includes an escaped Call-Info header field in the Refer-To header containing a reference URI that points to the EIDD data structure with a purpose parameter of "eidd".
12. The bridge returns a 202 Accepted message to the Primary PSAP.
13. The bridge then returns a NOTIFY message, indicating that subscription state of the REFER request (i.e., active).

[38] It is not ideal for the bridge to send the location of the caller in the INVITE, since the syntax of the Geolocation header would imply the location sent was that of the bridge, which is the UAC in the INVITE. Therefore, it is recommended that the bridge construct an EIDD that contains the location of the caller. For backwards compatibility with V1 of this document, the bridge may send Geolocation in the INVITE from the bridge to the primary PSAP.



One Nation 9-1-1 One Number

14. The Primary PSAP returns a 200 OK in response to the NOTIFY message.

#### 5.9.3.2 Bridge Invites the Secondary PSAP to the Conference

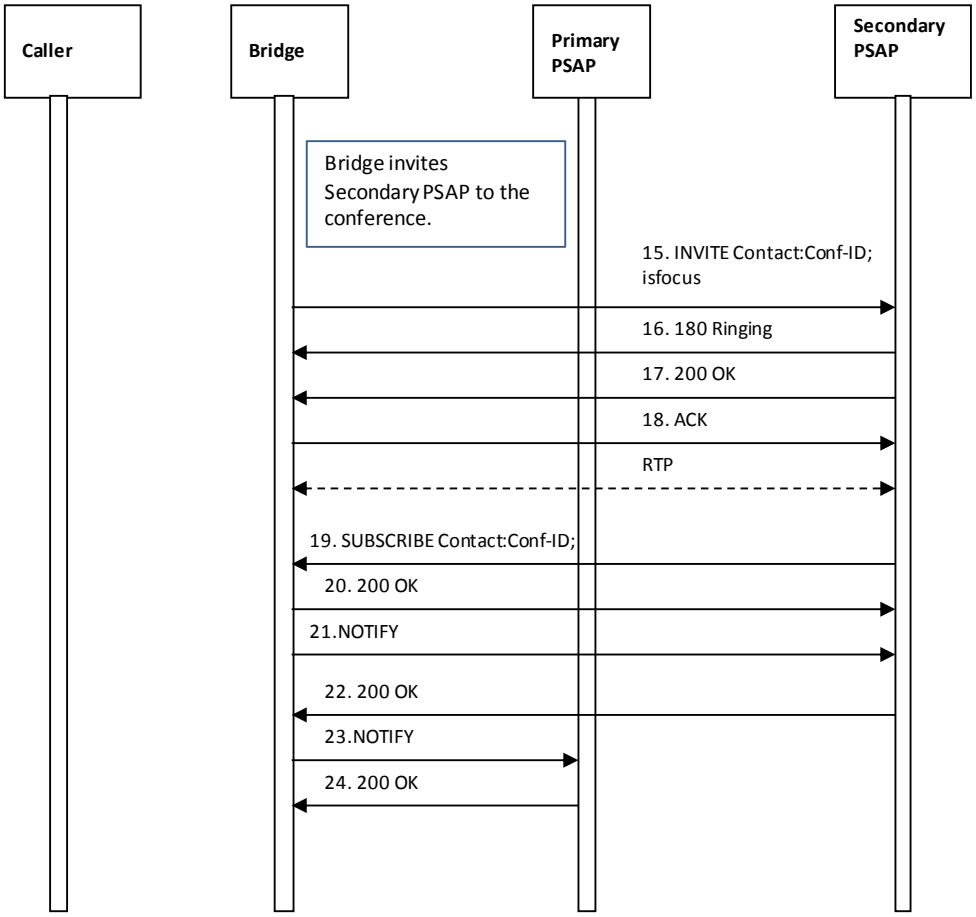



**Figure 5-12 Secondary PSAP Invited to Conference**

15. The bridge invites the Secondary PSAP to the conference by sending an INVITE method containing the Conf-ID and the isfocus feature parameter. The INVITE also contains a Call-Info header field containing a reference URI that points to the EIDD data structure and a purpose parameter of "eidd".
16. The Secondary PSAP UA responds by returning a 180 Ringing message to the bridge.
17. The Secondary PSAP 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 Secondary PSAP and the bridge.*

19. The Secondary PSAP subscribes to the conference associated with the Conf- ID provided in the INVITE message from the bridge by sending a SUBSCRIBE message to the bridge.
20. The bridge acknowledges the subscription request by sending a 200 OK message back to the Secondary PSAP.

21. The bridge then returns a NOTIFY message to the Secondary PSAP to provide subscription status information.
22. The Secondary PSAP responds by returning a 200 OK message.
23. The bridge sends a NOTIFY message to the Primary PSAP providing updated status for the subscription associated with the REFER request.
24. The Primary PSAP responds to the NOTIFY message by returning a 200 OK message.

    *At this point the caller, Primary PSAP, and Secondary PSAP are all participants in the conference.*

#### 5.9.3.3 Secondary PSAP Terminates the Call

When the Primary PSAP determines that it can drop from the bridge, it will follow the flow described in Section 5.8.1.4, steps 45 and 46. When the Secondary PSAP determines that the call should be terminated, it will follow the flow illustrated below.

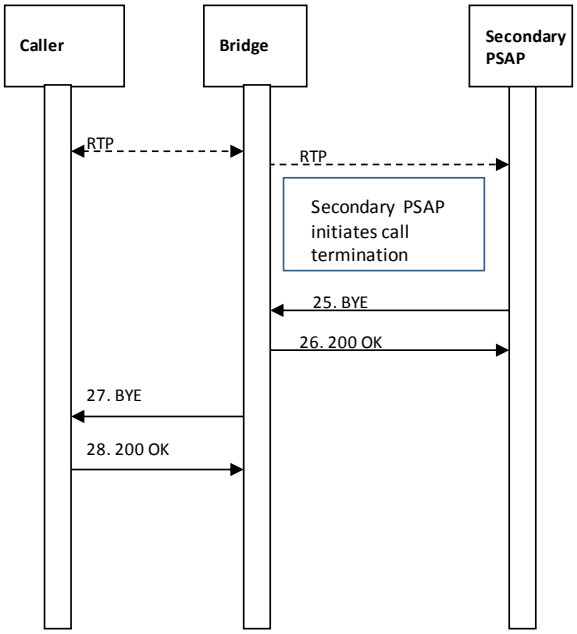



**Figure 5-13 Secondary PSAP Terminates Call**

25. Secondary PSAP initiates call termination by sending a BYE message to the bridge.
26. The bridge responds by returning a 200 OK message.

    *At this point, the session between the bridge and the Secondary PSAP is torn down.*

27. The bridge sends a BYE message to the caller's device.
28. The caller's device responds by returning a 200 OK message to the bridge.

    *At this point, the session between the caller and the bridge is torn down.*

The characteristics of this solution are:

- Media is anchored at the bridge regardless of what happens to the call.

- The bridge is always in the path regardless of whether the device implements Replaces or not.
- The original bridge is always in the path whether the Primary PSAP subsequently transfers the call or not. Receipt of the call on the bridge must trigger dial out of the call to the Primary PSAP/call taker.
- The bridge must populate the (original) caller location information received in the Geolocation header of the incoming INVITE message in the Geolocation header of the outgoing INVITE message to the Primary PSAP.
- The bridge must populate any Call-Info header fields received in the incoming INVITE message in the outgoing INVITE message to the Primary PSAP.
- Termination of the Secondary PSAP leg causes the bridge to (automatically) terminate the leg to the caller.
- Note that the call taker's system behaves differently in this scenario in that the initial call is received with an 'isfocus' feature parameter; the call taker need not establish a conference at the bridge if it determines that a transfer is necessary

### 5.9.4 Recommendations

BCFs should support option 1. This is the most likely scenario for most networks and has no impact or dependency on other elements. PSAP CPE may support option 2, which has no impact or dependency on other elements. PSAP CPE may support option 3 if the bridge support is available. Bridges may support Option 3. ESInet designers must decide which mechanism will be used on their network and all appropriate elements must support that mechanism. Consideration must be given to how calls will be transferred to or accepted from ESInets making different choices. Only ONE mechanism should be enabled. Other methods are acceptable provided that they do not assume/require support of Replaces by calling devices. Selection of a method to handle the lack of Replaces implementations in calling devices must take into account how overall system reliability goals are to be met, and specifically, how failures of various elements in the solution affect call reliability.

## 5.10 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 (OBO) 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. 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 [9], HELD Dereferencing (RFC 6753) [78], and/or SIP Presence Event Package [31]. 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 [102] and event rate control [112].

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 [77]. Using SIP Presence, the entity desiring location subscribes to the SIP Presence Event Package (RFC 3856 [31]) at the location URI provided[39]. The LIS sends NOTIFY transactions (RFC 3265 [17]) 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 [12] 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 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 [127]). Rate limits (RFC 6446 [112]) and Location filters (RFC 6447 [102]) are useful for this application and must be supported by the LIS if it supplies a SIP location URI[40].

A LIS must validate locations prior to entering them into the LIS using the LVF (see Section 5.3).

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. 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 LISs 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 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

[39] 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.

[40] 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.

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.

### 5.11 Additional Data Repository (ADR)

The Additional Data Repository is a database that holds Additional Data. URIs pointing to the ADR may be passed in a call, in an EIDD or by other mechanisms. The ADR returns an XML data structure in response to an HTTPS GET of the URI.

An emergency call must have at least two[41] Call-Info header fields each with a URI that resolves to an Additional Data structure [143] (the required block types are EmergencyCallData.ProviderInfo and EmergencyCallData.ServiceInfo). The URI may resolve to a Content Identifier that references the body of the INVITE message where the Additional Data may be found, or it may lead to an external database. Additionally, the <provided-by> element of a PIDF-LO may contain an Additional Data URI or the content of a set of Additional Data blocks. 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 origination networks in the ALI.

All origination networks and service providers[42] are expected to provide at least this minimum set of information which must be populated in an ADR when passed by reference, or provided in the body of the INVITE message when passed by value. Access networks are expected to provide the same minimum set of information. The ADR is queried with the URI obtained from the Call-Info header field with a purpose starting with "EmergencyCallData.", or in a <provided-by> of a PIDF-LO and returns the Additional Data structure [143]. It is important that ALL origination networks and service providers handling the call add a Call-Info header field, where the origination network or service provider can be reasonably expected to determine they are handling an emergency call. 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.

ADR servers are not required to be able to serve a query more than 5 minutes after an emergency call is terminated.

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 303 response (Iterative Refer).

---

[41] Wireline and other legacy networks that historically provide subscriber information are expected to continue to do so using the SubscriberInfo block of Additional Data.

[42] 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.



One Nation 9-1-1 One Number

Devices such as those within telematics equipped vehicles and medical monitoring devices that can place emergency calls could have the capability to respond to an ADR query, or could publish data to an external ADR that would respond to dereference requests. A service provider (such as a telematics service provider) may provide the ADR instead of the device. Other devices may also provide an ADR for use in an emergency call. Alternatively, the data may be provided by value by the device, originating network or service provider.

The ADR could be provided by the access network, origination network or service provider. For service providers, access and origination networks that only provide the minimal data called for in [143], the ADR could be provided by a third party. For Additional Data provided by the calling entity itself, the ADR could be provided by it, 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 5.11.1 for specifications for this capability.

### 5.11.1 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 5.11.

The IS-ADR provides a web service. When queried with caller's "From" address or P-Asserted-Identity (as retrieved from the SIP header)[43], the IS-ADR returns one of the following in response:

- An XML document containing the caller's Additional Data (by value).
- A URI that can be used to dereference the caller's Additional Data.
- A HTTP 303 response (Iterative Refer), 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.

**IS-ADRRequest**

| Parameter | Condition | Description |
|---|---|---|
| callerURI | Mandatory | URI of caller From/P-A-I |

**IS-ADRResponse**

| Parameter | Condition | Description |
|---|---|---|

[43] 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.

| Parameter | Condition | Description |
|---|---|---|
| AdditionalDataValue | Conditional, must be present if AdditionalDataReference is not provided | Caller data value |
| AdditionalDataReference | Conditional, must be present if AdditionalDataValue is not provided | Caller data URI |
| statusCode | Mandatory | Status Code |

Status Codes

200 Okay No error

526 No Data Found

504 Unspecified Error

It is anticipated that a number of third parties will choose to host an IS-ADR. A registry of recognized IS-ADRs is defined by this document (Section 11.22). PSAPs and other responsible parties can then use the NENA IS-ADR registry as input into the configuration of the NG9-1-1 functional elements under their control.

### 5.12 Interactive Media Response system (IMR)

The IMR is similar to an Interactive Voice Response (IVR) unit, but handles audio, video and text media. It may be used to answer calls when the PSAP is receiving more calls than it has call takers to answer them. It offers interaction with the caller ("Press 1 if this about the car crash on Fourth and Main, Press 2 if this is about some other problem").

IMRs must implement RFC 4240 [43], and VXML V2.0 [133]. VXML <audio> tags must specify multiple MIME types with appropriate types for the media. Synthesis scripts must render text for text media. The IMR must implement at least the codecs listed in Section 4.1.8.

The syntax for specifying a URI to route to a specific VXML script is defined in RFC 4240.

Calls may be queued within the IMR waiting for available call takers. The queue of calls must be a queue as defined in 5.2.1.2 and maintain the specified queueState and DequeRegistration events so that PSAP management can monitor and control the queue as it does all other queues.

IMRs must interpret an IM, RTT or other text received consisting the digits 0-9, '#' or '*' immediately following a prompt for input as equivalent to DTMF key presses.

IMRs must implement the Session Recording Client interface defined by SIPREC [153]. Provisioning may control whether the IMR logs media.

Each FE in the IMR must implement the server-side of the ElementState event notification package. The IMR must promptly report changes in its state to its subscribed elements.

The set of IMR FEs within an ESInet must implement the server-side of the ServiceState event notification package for the IMR. Since IMR is typically a local service it is recommended that each NGCS that provides an IMR service implement ServiceState for that NGCS.

## 5.13 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. 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 logger" 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.

### 5.13.1 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) interface ([153]) for recording the media and associated metadata, and provide a Real Time Streaming Protocol (RTSP) (RFC 2326 [134]) interface to play back the media. The web service includes the functions described in the LogEvent section.

Clients to the logging service must support logging to at least two loggers for redundancy purposes, with support for three (3) or more desirable. The logging service is NOT intended to support other kinds of devices that may wish to operate from the LogEvent records. See LogEventReplicator, Section 5.13.6.

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 an IMR service implement ServiceState for that NGCS.

Note: Need recommendations on siprec metadata to improve interoperability, noted for future work.

### 5.13.2 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 [153]. The Logging Service must implement the SRS interface. Any element that has call media, including

MSRP, 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) and 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 [153] 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.

The logging recorder that supports the Session Recording Server (SRS) functionality defined in the SIPREC specification [153] interfaces to any Functional Elements that support a Session Recording Client (SRC).

The SRC and the Logging Service acting as the SRS must support the SIPREC Metadata interface [154]. The Logging Service creates a SiprecMetadata LogEvent to log this metadata (see the LogEvent section for details). Each emergency call (that is, each Communication Session), must result in a separate Recording Session.

All SRCs and SRSs 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 SRSs.

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.

#### 5.13.2.1 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

- Both parties communicate
- Caller hangs up
- Answer-Point hangs up
- SRC closes the recording session.

Note: All additional information about the call can retrieved from the logging service using the call identifier.

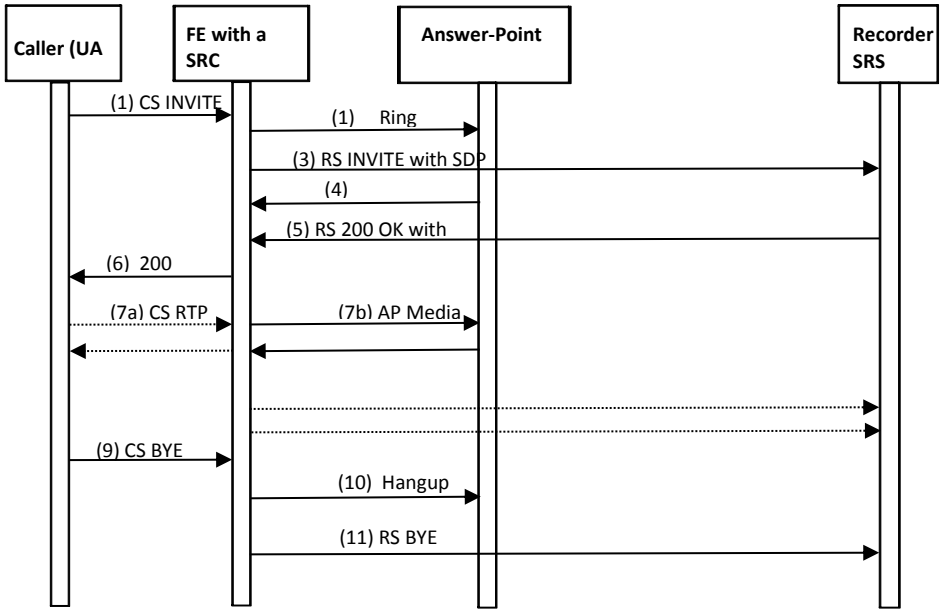



**Figure 5-14 Incoming Call**

### 5.13.2.2 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 retrieved from the logging service using the call identifier.

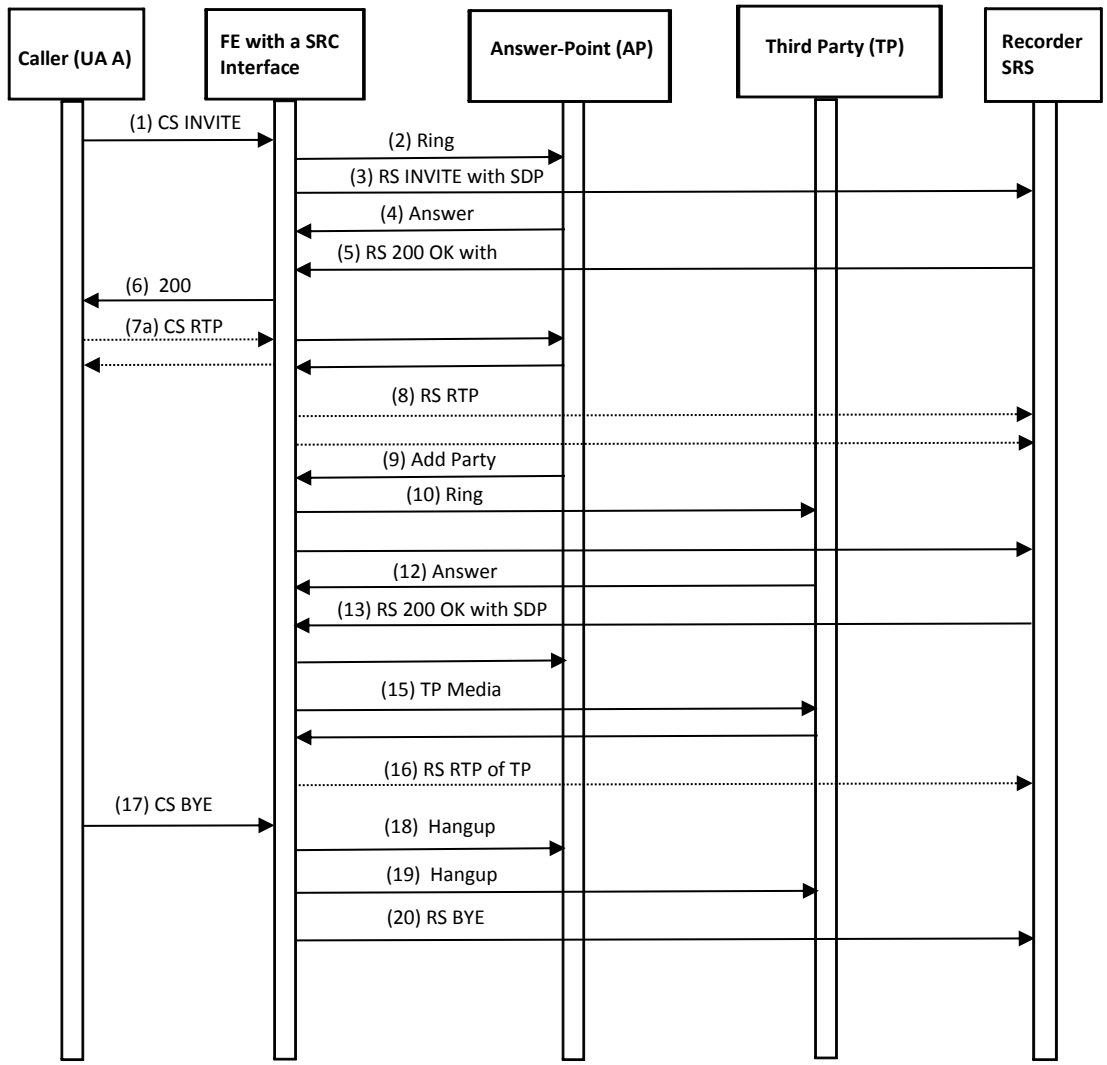



**Figure 5-15 Three Party Call**

#### 5.13.2.3 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 retrieved from the logging service using the call identifier.

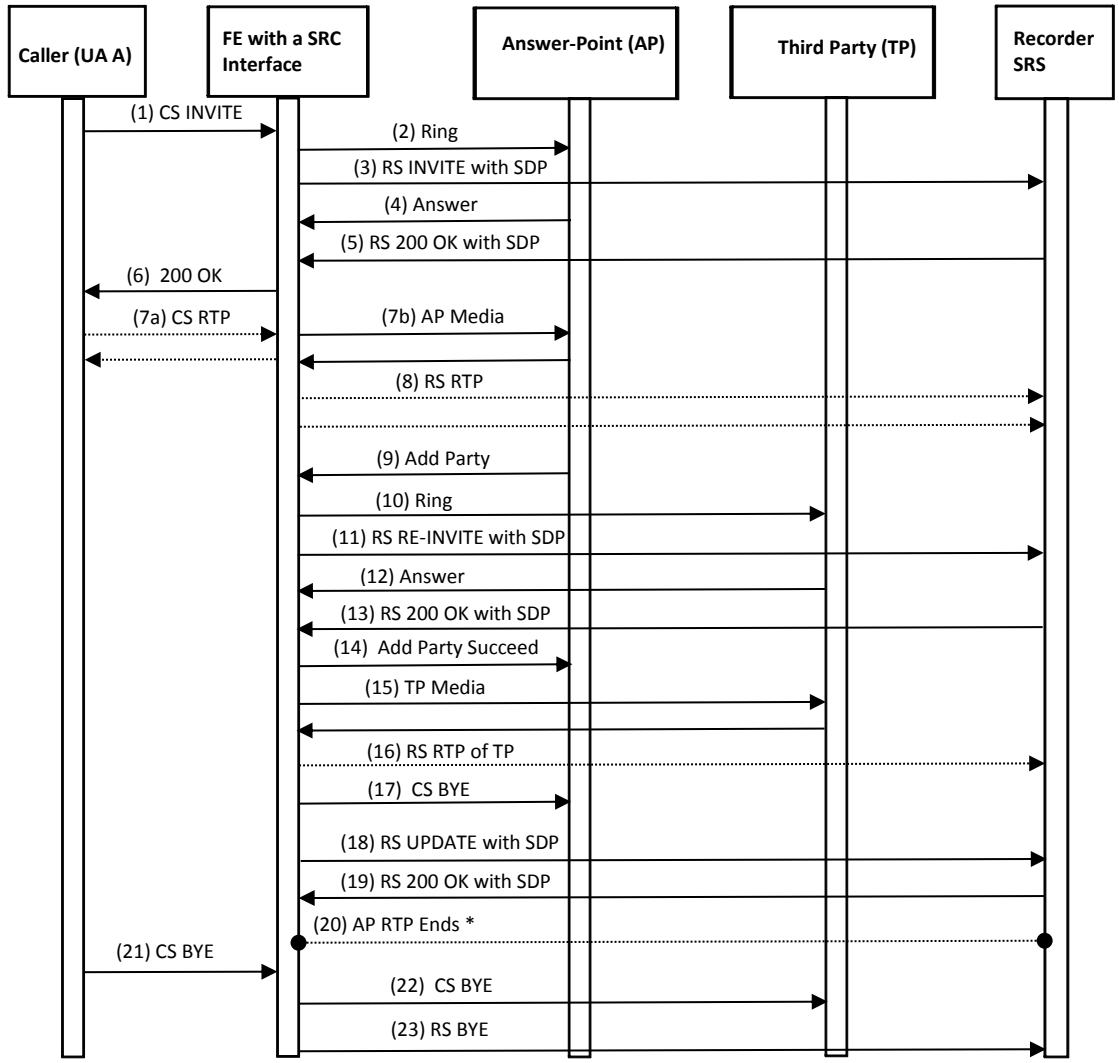



**Figure 5-16 Attended Transfer**

* RTP stream from Answer Point to Recording Server in Step 8 stops.



One Nation 9-1-1 One Number

#### 5.13.2.4 Call Back (Outgoing Call)

The SRC initiates an outbound call via recorded administrative line in response to a 911 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 retrieved from the logging service using the call identifier.

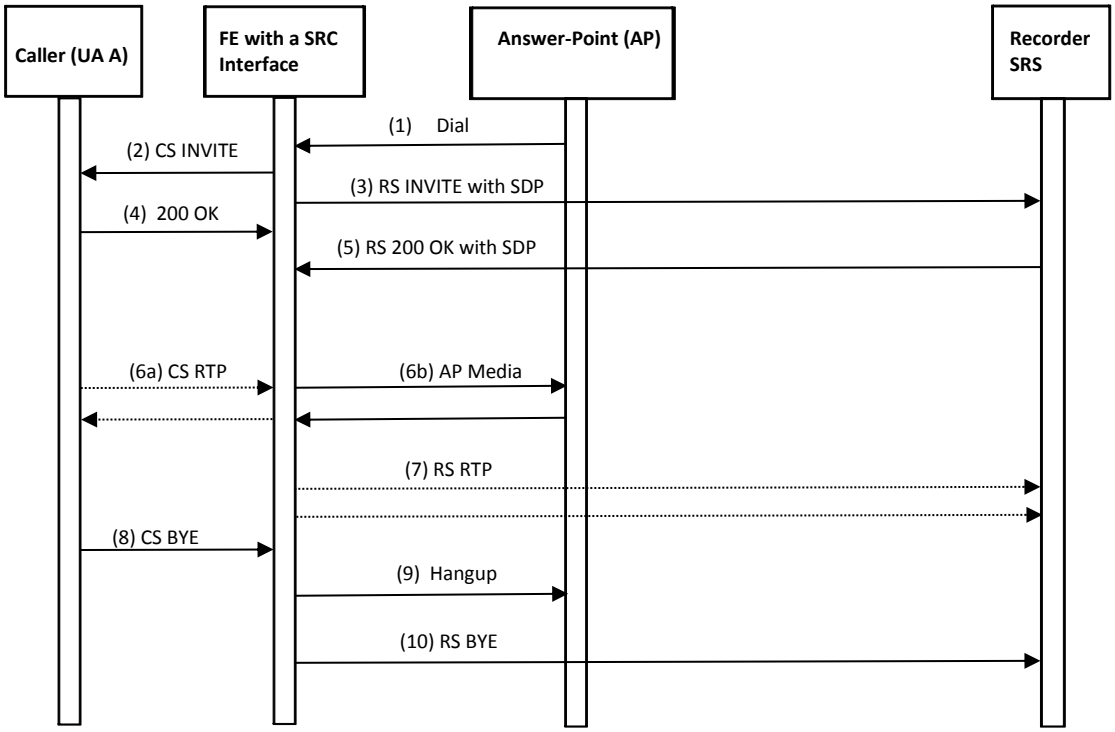



**Figure 5-17 Call Back**

#### 5.13.2.5 Blind Transfer

The Answer-Point transfers 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 retrieved from the logging service using the call identifier.

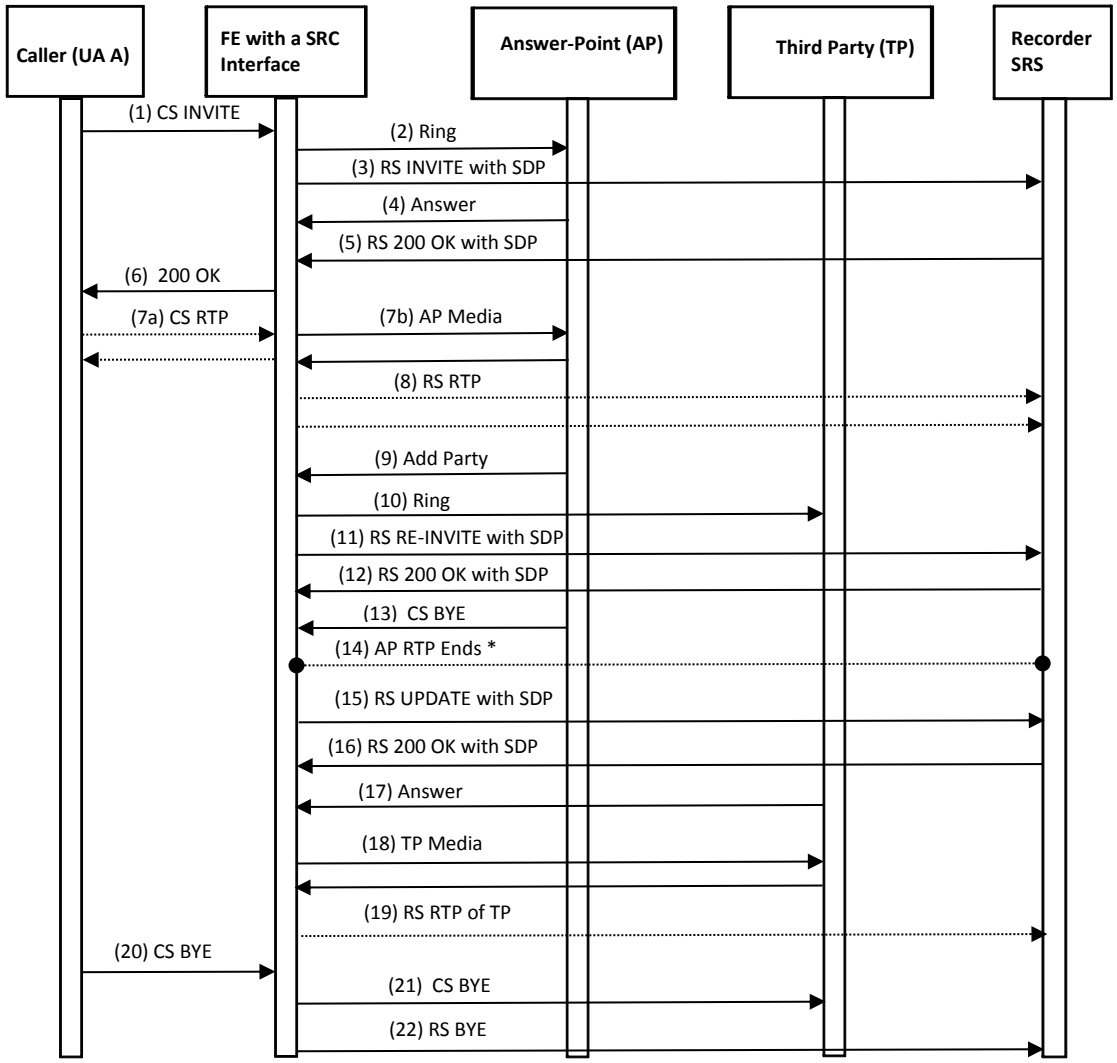



**Figure 5-18 Blind Transfer**

### 5.13.2.6 Clean Logging Service Shutdown

The Logging Recorder must be able to provide a clean shut down by sending a BYE as specified in Section 4.1.1.3, 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 retrieved from the logging service using the call identifier.

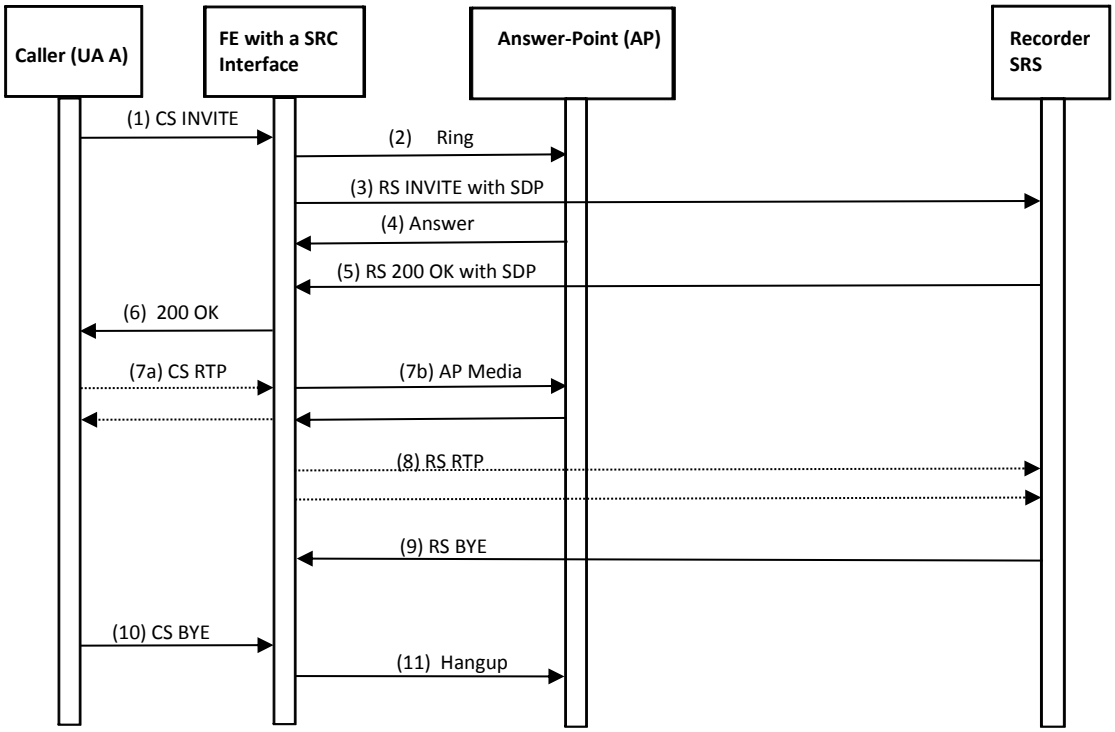



**Figure 5-19 Logging Service Shutdown**

### 5.13.3 Log Recording

#### 5.13.3.1 LogEvent Request

LogEvent logs an event into the Logging Service. The LogEvent request includes the following parameters:

| Parameter | Condition | Description |
|---|---|---|
| LogEventTimestamp | Mandatory | A Timestamp as defined in Section 3.3 |
| AgencyId | Conditional, must be supplied if ElementId not supplied, may be supplied otherwise | AgencyId of the agency that logged the event |
| ElementId | Conditional, must be supplied AgencyId not supplied, may be supplied otherwise | ElementId of the element that logged the event |

| Parameter | Condition | Description |
|---|---|---|
| AgencyAgentId | Conditional, if the log record is traceable to an agent, must be provided. If the log record is only attributable to an element or agency, this element will not be included. | The agentId (Section 3.1.1) of an agent at the agency listed in the AgencyId tag, see Section 3.1.2. |
| AgencyPositionId | Optional | Identifier for the position that is handling a call. |
| CallIdURN | Conditional, must be supplied if event is associated with a call | The call identifier of a call, see Section 3.1.5 |
| IncidentIdURN | Mandatory | The Incident Tracking Identifier associated with the call, see Section 3.1.6 |
| SIPCallId | Conditional, must be supplied if event is associated with a SIP call | CallId from SIP |
| OtherElementAddress | Conditional. Must be supplied 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 participates in a transaction that triggered this LogEvent (i.e., an element that sent or responded to a query). This is not the address of the element that logs the event. IP address and port must be logged if known<ref IPv6 format statement>. |
| EventValuesCode | Mandatory | Type of log record |

Digital signatures will be considered in a future revision of this document.

The CallIdURN and IncidentIDURN 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 logger will need to track such messages (via the SIP call identifier) and log the Call and Incident IDs.

The LogEvent object contains an extension point that may be used to log any proprietary data in a logger. The namespace that defines the extension is included in the LogEvent object and the LogEvent may contain any object defined in that namespace. Each LogEvent defined in this document contains an extension point for that LogEvent, which allows logging of additional

proprietary data. 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 a whitelist or blacklist 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.

#### 5.13.3.2 LogEvent EventTypes

Note: In the EventTypes described below there is a very large amount of logging, including cases where information is logged at both the sender and receiver. Future revisions of this document will describe a way to control what must be logged.

The following EventTypes are defined in this document:

CallProcess: 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 CallProcess event. There are no parameters to "Call Process". Elements that log CallProcess also log the actual SIP message with CallSignalingMessage.

StartCall/EndCall: Each element that is call stateful logs the beginning and end of its processing of a call, including non-human-initiated calls, with Start Call and End Call events. Elements that log StartCall/EndCall must also log the actual SIP message with CallSignalingMessage for SIP parts of a call and GatewayCallEvent for TDM parts of a call. For StartCall and EndCall, the Timestamp must be the time the INVITE, MESSAGE, BYE or equivalents to these messages, or the final error code was received or sent by the element logging the event. Both StartCall and EndCall must be logged upon receipt of MESSAGE. A <CallDirectionValuesCode> tag has one of two values "incoming" and "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 <StartCallStandardPrimaryCallType>, <StartCallStandardSecondaryCallType> and <StartCallLocalCallType> tags may be included in StartCall. The <StartCallStandardPrimaryCallType> and <StartCallStandardSecondaryCallType> tags are limited to values found in the LogEvent Call Type Registry [11.16] <StartCallLocalCallType> can have any value defined locally. Optional <StartCallLocalUse> elements are also available (limited to 128 bytes each). When StartCall is used with non-SIP interfaces, <to> and <from> tags are used to capture the participants in the call.

StartRecCall/EndRecCall is identical to StartCall/EndCall, but is logged by the logging service (SRS) and the client (SRC) for the siprec recording session.

TransferCall: 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 <TransferCallTarget> tag. Elements that log TransferCall must also log the actual SIP <TransferCallTargetSipCallId> tag 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.

Note: Mechanisms to support blind and supervised transfer are not defined in this document and will be standardized in a future revision of this document. Logging of such transfers is still required.

Route: Proxy servers that make routing decisions (ESRPs or other SIP proxy servers in the path of the call) log the route it selected with the Route EventType. The URI where it decided to send the call (encoded in a <RouteUri> tag, plus a text string <RouteReason> for choosing that route are included in the LogEvent. For ESRPs, the name of the rule is included in a <RouteRule> tag.

StartMedia: StartMedia contains information about one call medium (voice, video or RTT/MSRP text). The media event includes a text string <SessionDescriptionProtocol> tag that contains an RFC 2327 Session Description Protocol [55] description of the media codecs as negotiated. The StartMedia event must include one or more <MediaLabel> tags that must match the SDP labels if they exist. More than one Media event 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 call back, bridge or BCF if the BCF anchors media) when at the start of media reception or transmission as appropriate. A <DirectionValuesCode> tag has one of two value "incoming" and "outgoing".

EndMedia:EndMedia signals that media streams stopped. The EndMedia event must include one or more <MediaLabel> tags that must match the SDP labels in the corresponding StartMedia event. More than one EndMedia (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 call back, bridge or BCF if the BCF anchors media) for the communication session media. A <MediaQualityStats> tag contains tags that give QoS statistics about the media stream. The content of <MediaQualityStats> contains the "SessionReport" element from RFC 6035. <MediaQualityStats> should be supported by all media anchors.

StartRecMedia and EndRecMedia are identical to StartMedia/EndMedia but apply to the SIPREC recording session. Both the SRC and SRS log StartRecMedia/EndRecMedia. If an entity receives a media stream where 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 StartRecMedia for it. The <MediaLabel> tags must be the same as those in the StartMedia/EndMedia 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> tag is used in this case containing the RFC 4575 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.

RecordingFailed: Indicates that the entity logging this event attempted to record media, but the media recording mechanism failed. Contains an SDP description of the media that failed to be recorded in a <SessionDescriptionProtocol> tag, and <RecordingFailedReasonCode> and <RecordingFailedReasonText> parameters that specifies why recording could not complete. <RecordingFailedReasonCode> must be a value from the ReasonCode registry defined in Section 11.24. The Session Recording Client in a SIPREC media recording session is responsible for logging this event.

Message: A SIP Message is logged with a Message log event. Elements that log Message must also log the actual SIP message with CallSignalingMessageThe text of the message is included as a

<text> parameter. A <direction> tag has one of two value “incoming” and “outgoing”. MSRP is logged with SIPREC.

AdditionalAgency: When an agency becomes aware that another agency may be involved, in any way, with a call, it must log an AdditionalAgency event. The AdditionalAgency event includes an <AdditionalAgencyId> tag which is an Agency Identifier (see Section 3.1.1). 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.

MergeIncident: 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 MergeIncident. The MergeIncident record contains the IncidentId of the incorrectly assigned incident in the <IncidentIDURN> tag in the header of the log record, and the Incident Id of the actual Incident in an <MergeIncidentId> tag. After a merge, the Id in the <MergeIncidentId> tag 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.

UnMergeIncident: when a MergeIncident is found to have been done in error, UnMergeIncident will undo the operation. The UnMergeIncident record contains the IncidentId of the Merged incident in the <IncidentIDURN> tag in the header of the log record, and the Incident Id of the other Incident in a <UnMergedFromIncidentId> tag.

LinkIncident: Incidents are linked when two different incidents are not the same real world event, but are related in some way. The LinkIncident record contains the Incident Tracking Identifier of the new Incident in the <IncidentIDURN> tag in the header, and the Incident Tracking Identifier of the original Incident being linked to in a <LinkedIncidentId> tag. The <RelationshipValuesCode> tag specifies the relationship between the incidents. Values include “parent”, “child”, “peer” and “unspecified”. For “parent” and “child”, the IncidentIDURN in the header is the one described by the <RelationshipValuesCode> tag.

UnLinkIncident: when a LinkIncident is found to have been done in error, UnLinkIncident will undo the operation. The UnLinkIncident record contains the IncidentId of the Linked incident in the <IncidentIDURN> tag in the header of the log record, and the Incident Id of the other Incident in an <UnlinkedFromIncidentId> tag.

ClearIncident: When an agency finishes its handling of an Incident, it logs a ClearIncident record. Other agencies may still be processing the Incident.

ReopenIncident: If an agency needs to log events on an Incident that it has logged a ClearIncident for, it logs a ReopenIncident.

LoSTquery: Both the element that queries the ECRF/LVF and the ECRF/LVF itself generate a LoSTquery LogEvent. The LogEvent includes the entire LoST query in the <LoSTQueryAdapter> tag. A <DirectionValuesCode> tag has one of two value “incoming” and “outgoing”. The ECRF/LVF will obtain the CallIdURN and IncidentIDURN from the LoST extension defined in Section 11.28. A <LoSTQueryId> tag is used to relate the request to the response. The id is

generated locally, must be globally unique, and it is suggested it be of the form: "urn:nena:uid:logEvent:<locally unique id>". If the element is logging a malformed query it has received, it includes it in a <LoSTMalformedQuery> tag.

LoSTresponse: Both elements that query the ECRF/LVF, and the ECRF/LVF itself generate the LoSTresponse. The entire response is logged using a <LoSTResponseAdapter> tag. Malformed, invalid or responses not received from the server are logged in a <ResponseError> tag that contains an error code from the Error Codes Registry (Section 11.28). A <DirectionValuesCode> tag has one of two values: "incoming" and "outgoing". A <LoSTResponseId> tag is used to relate the request to the response, and must match the id used in the LoSTquery LogEvent. If the element is logging a malformed response it has received, it includes it in a <LoSTMalformedResponse> tag.

CallSignalingMessage: Call Signaling (e.g. SIP) messages are logged with the CallSignalingMessage LogEvent. The entire message is included in a <CallSignalingMessageText> tag. A <DirectionValuesCode> tag has one of two values: "incoming" and "outgoing". An element must always log messages it receives (with <DirectionValuesCode> 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 <DirectionValuesCode> set to "outgoing") if it changes any part of the signaling message. An element must log outgoing messages it originates. A <CallSignalingProtocol> tag indicates the protocol. Absence of the <CallSignalingProtocol> tag defaults to "sip". A registry of protocol values is defined in Section 11.15.

SiprecMetadata: the Logging Service must create LogEvents for any metadata received via the siprec metadata interface [154]. It does this by logging a SiprecMetadata LogEvent to itself. The metadata is included a <SIPRECMetadataText> tag. The Logging Service must fill in the header fields for which the values are known, such as the CallIdURN and IncidentIDURN supplied by the Session Recording Client. The sipCallId in the header will be set to the SIP callid from the communication session, not the SIP callid from the recording session.

ALILocationQuery: an LSRG [151] logs the query it sends to or receives from an ALI server with the ALILocationQuery LogEvent. 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 <ALILocationQueryText> tag, and any message delimiter control characters such as STX/ETX are not included. The CallIdURN and IncidentIDURN, 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> tag has one of two value "incoming" and "outgoing". An <ALILocationQueryId> tag is used to relate the request to the response. The id is generated locally, must be globally unique, and it is suggested it be of the form: "urn:nena:uid:logEvent:<locally unique id>".

ALILocationResponse: an LSRG must log the response it sends to or receives from its query to an ALI server with the ALILocationResponse LogEvent. 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 <ALILocationResponseText> tag, 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 <ResponseError> tag that contains an error code from the Error Codes Registry (Section 11.28). The CallIdURN and IncidentIDURN may be left blank if they are not known by the LSRG. A <DirectionValuesCode> tag has one of two values: "incoming" and "outgoing". An

<ALILocationQueryId> tag is used to relate the request to the response, and must match the id used in the ALILocationQuery LogEvent.

MalformedMessage: an element that receives a malformed SIP message logs it with the MalformedMessage LogEvent. The malformed message is included in a <SIPMessageText> tag. An <IPAddress> tag is included, which contains the IP address of the sender of the message. An optional <MalformedMessageExplanationText> tag 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.

SplitIncident: 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 SplitIncident LogEvent. SplitIncident requires the agency splitting the incident to create two records, one with the old Incident Id in the header and the new Incident Id in the tag, and another SplitIncident record with the new Incident Id in the header and the old one in the tag. The old or new Id is included in a <SplitIncidentIdURN> tag, which contains the Id and an "oldOrNewValuesCode" attribute that specifies whether this tag contains the old Id or the new Id.

EIDD: any element that sends or receives an Emergency Incident Data Document [148] must log it with the EIDD LogEvent. If the EIDD is sent by value, the value is logged in an <EIDDBody> tag. If an EIDD is sent or received by reference, the EIDD URI must be logged with an <EIDDReference> tag. When the URI is dereferenced, another EIDD LogEvent must be created with the <EIDDReference> and <EIDDBody> by both the client and server. A <DirectionValuesCode> tag has one of two values: "incoming" and "outgoing".

DiscrepancyReport: 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 received with the DiscrepancyReport LogEvent. The body of the report or response is included in a <DiscrepancyReportContents> tag. A <DirectionValuesCode> tag has one of two values: "incoming" and "outgoing". An <DiscrepancyReportFunctionValuesCode> tag 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.

ElementStateChange: when an element sends a notification of state change as described in the Element State section of this document, it must log the ElementStateChange LogEvent. The event contains the body of the notification message in a <StateChangeNotificationContents> tag. Elements that receive changes in elementState may log receipt of such changes. The new state is logged with <StateChangeNotificationContents> tag. The element ID (FQDN) of the element whose state changed is logged in the <AffectedElementId> tag. This tag is optional if the element that provides the state change is the element whose state is changed. A <DirectionValuesCode> tag has one of two values "incoming" and "outgoing". Note that a Call Identifier, SIP Call Id and Incident Tracking Identifier usually won't be available for an ElementStateChange. Devices that have proprietary interfaces may implement ElementStateChange 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 ElementStateChange.

ServiceStateChange: when a Service sends a notification of state change as described in the Service State section of this document, it must log the ServiceStateChange LogEvent. Elements that receive changes in serviceState may log receipt of such changes. The new state is logged with <StateChangeNewStateValue> tag. The service ID (FQDN) of the service whose state changed is logged in the <StateChangeAffectedServiceId> tag. A <DirectionValuesCode> tag has one of two values “incoming” and “outgoing”. Note that a Call Identifier, SIP Call Id and Incident Tracking Identifier usually won’t be available for a ServiceStateChange.

AdditionalDataQuery: a query for Additional Data may be logged with the AdditionalDataQuery LogEvent. The URI the request was sent to is logged in a <AdditionalDataQueryUri> tag. The event contains the body of the query in a <AdditionalDataQueryText> tag. 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 they receive. A <DirectionValuesCode> tag has one of two values “incoming” and “outgoing”. An <AdditionalDataQueryId> tag is used to relate the request to the response. The id is generated locally, must be globally unique, and it is suggested it be of the form: “urn:nena:uid:logEvent:<locally unique id>”.

AdditionalDataResponse: any Additional Data that is retrieved by a client must be logged using the AdditionalDataResponse LogEvent. The body of the retrieved data is included in <AdditionalDataResponseText> tags, one per block of Additional Data. Malformed, invalid or responses not received from the server are logged in a <ResponseError> tag that contains an error code from the Error Codes Registry (Section 11.28). 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 they send. A <DirectionValuesCode> tag has one of two values: “incoming” and “outgoing”. An <AdditionalDataQueryId> tag is used to relate the request to the response, and must match the id used in the AdditionalDataQuery LogEvent.

LocationQuery: a HELD dereference request [78] or SIP Presence SUBSCRIBE message [31] may be logged with the LocationQuery LogEvent. The URI the request was sent to is logged in a <LocationQueryUri> tag. The body of the request or SUBSCRIBE is included in a <LocationQueryText> tag. 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 <DirectionValuesCode> tag has one of two values: “incoming” and “outgoing”. An <LocationQueryId> tag 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 it be of the form: “urn:nena:uid:logEvent:<locally unique id>”.

LocationResponse: a HELD dereference response, a SIP Presence NOTIFY message and a re-INVITE with a new location are logged with the LocationResponse message. The body of the response or message is included in a <LocationResponseText> tag. Malformed, invalid or responses not received from the server are logged in a <ResponseError> tag that contains an error code from the Error Codes Registry (Section 11.28). 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 <DirectionValuesCode> tag has one of two values “incoming” and “outgoing”. An

<LocationQueryId> tag is used to relate the request or subscription to the response or notifications, and must match the id used in the LocationQuery LogEvent.

CallStateChange: 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 <CallStateText> tag. The CallIdURN, IncidentIDURN and sipCallId in the header are from the emergency call whose state has changed. For state changes that involve another "leg" of a call, such as AddParty, a <CallStateLegCallId> tag 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. CallStateChange must be logged by all elements that change the state of the call, which would include a bridge and all entities within the ESInet that request bridge actions when an emergency call is on a bridge. A <DirectionValuesCode> tag 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, the identifier of the target whose state changed must be included in a <CallStateTargetId> tag. If the target is a SIP device, this must be the sip URI of the target. An optional <CallStateChangeReason> tag contains the reason why the state changed. The content of this tag is not standardized at this time. This document creates a registry for these call states Section 11.17.

GatewayCallEvent: used by an LNG, LPG or LSRG to log a call entering or leaving it on a legacy interface. Contains the following parameters which are optional, but must be included if known:

- GatewayCallPortTrunkGroup – the port or trunk group
- GatewayCallpANI - 10-digit number when LNG or LSRG handles a call from a legacy wireless or legacy VoIP network, or the pANI an LPG creates.
- GatewayCallDigits – 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.
- DirectionValuesCode - "incoming" or "outgoing"
- GatewayCallSignalingProtocol - "SS7" or "CAMA"
- GatewayCallLegacyCallId

Hookflash: an LPG logs a "hookflash" event with the Hookflash LogEvent. An identifier for the line where the event occurred is included in a <HookflashLineId> tag, which is optional but must be provided if known. Not used when already logged as part of a GatewayCallEvent

LegacyDigits: an LPG logs DTMF or MF digits with the LegacyDigits LogEvent. A <SentOrReceivedValuesCode> tag, with values of "sent" or "received", identifies the direction of the digits. A <DigitsTypeValuesCode> tag, with a value of "DTMF" or "MF" identifies the type of digits that were received. <DigitsContentString> carries the digit or digits that were transmitted or received. Not used when already logged by GatewayCallEvent (such as sending pANI digits at an LPG).

AgentStateChange: an element logs a change in agent device state with the AgentStateChange LogEvent. There are two tags <PrimaryAgentStateValuesCode> and <SecondaryAgentState>.

<PrimaryAgentStateValuesCode> has two values, Available and Not Available. This document creates a registry for secondary agent device states [11.20]. If the device whose state has changed is not the element identified in the header, the identifier of the device must be included in a <DeviceID> tag. All elements supporting agents must support the <PrimaryAgentStateValuesCode>, <SecondaryAgentState> support is optional.

Several of these secondary states (e.g. Active and Hold) make sense with both Available and Not Available primary states.

QueueStateChange: a queue manager must log a change in the state of the queue with the QueueStateChange LogEvent. The event contains the body of the notification message in a <StateChangeNotificationContents> tag. 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> tag. A <DirectionValuesCode> tag has one of two values: "incoming" and "outgoing". Note that a Call Identifier, SIP Call Id and Incident Tracking Identifier usually won't be available for a QueueStateChange.

SecurityPostureStateChange: an element or service must log a change in its security state with the SecurityPostureStateChange LogEvent. The event contains the body of the notification message in a <StateChangeNotificationContents> tag. Elements that receive changes in Security Posture state may log receipt of such changes. The element or service ID (FQDN) of the element or service whose security posture changed is logged in the <AffectedEntityId> tag. This tag is optional if the element that provides the state change is the element whose state is changed. A <DirectionValuesCode> tag has one of two values: "incoming" and "outgoing". Note that a Call Identifier, SIP Call Id and Incident Tracking Identifier usually won't be available for a SecurityPostureStateChange.

KeepAliveFailure: The OPTIONS request is the "keep alive" mechanism specified in this document (Sec. 4.1.2.3). An element that gets a normal response to its OPTIONS request does not log the response. But malformed, invalid or responses not received from the other element must be logged in a <ResponseError> tag that contains text and an error code from the Error Codes Registry (Section 11.28). There is a TimeOut error in that registry that is used for a timeout failure of OPTIONS.

This document creates a registry for LogEvents. See Section 11.14.

Note: A description of which elements generate which log event types will be described in a future revision of this document.

LogEvent function assigns a globally unique LogIdentifier to each LogEvent and returns the LogIdentifier in its response. The form of a LogIdentifier is a URI consisting of the string "urn:nena:uid:logid:", a unique string, the ":" character and the domain name of the Logging Service. The unique string must be between 10 and 35 characters long and unique to the Logging Service. An example LogIdentifier is "urn:nena:uid:logid:0013344556677-231:logger.state.pa.us". The domain specified must be the domain of the Logging Service to which the appropriate RetrieveLogEvent can be sent.

#### 5.13.3.3 LogEvent Response

The LogEvent Response includes the following parameters

| Parameter | Condition | Description |
|---|---|---|
| LogIdentifier | Mandatory | The identifier assigned by the logging service to the Log Event |
| statusCode | Mandatory | Status Code |

Status Codes

200 Okay

527 Bad Log Event

528 Event too big

529 Event not on whitelist

530 Event on blacklist

### 5.13.4 Log Retrieval

#### 5.13.4.1 RetrieveLogEvent

To retrieve a logged event from the Logging Service, RetrieveLogEvent will return the log record for all events. The request to RetrieveLogEvent includes a <LogIdUrn> parameter containing the LogIdentifier that was generated for the original LogEvent.

When the event is a StartRecMedia event, the returned event from RetrieveLogEvent will have one or more <RtspUri> parameters inserted by the logging service that must be RTSP URIs. The RTSP URI can be used to play back the call session. The <SessionDescriptionProtocol> and <MediaLabel> are also returned to indicate which media stream in the session the event refers to. These RtspUri 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.

A <MessageResult> is also returned from RetrieveLogEvent that can include:

Error Codes

200 Okay No error

519 No such logIdentifier

504 Unspecified Error

Policy shall control who can retrieve logged events from the Logging Service. The policy of the element/agency that logged the event governs what entities can retrieve the event.

#### 5.13.4.2 RetrieveTextConversation

Returns an HTML formatted record suitable for human consumption of the text portion of a call, including all text sent by all parties. A label preceding the text sent identifies the sender of the text. A time stamp of the start of the text is included in the label. A <CallIdURN> tag is in the request and



One Nation 9-1-1 One Number

a <RetrieveConversationText> tag in the response contains the html. A <MessageResult> is also returned that can include:

200 Okay No error

516 No such callIdentifier

504 Unspecified Error

#### 5.13.4.3 ListLogEventsByCallId

Returns a list of LogIdentifiers that have a specified Call Identifier. The request includes the <CallIdURN>. The response includes zero or more <LogIdURN>(s). A <MessageResult> is also returned that can include:

200 Okay No error

516 No such callIdentifier

504 Unspecified Error

#### 5.13.4.4 ListLogEventsByIncidentId

Returns a list of LogEvents that have a specified Incident Tracking Identifier. The request includes the <IncidentIdURN>. The response includes zero or more <LogIdURN>(s). A <MessageResult> is also returned that can include:

200 Okay No error

517 No such incidentIdentifier

504 Unspecified Error

#### 5.13.4.5 ListCallsbyIncidentId

Returns a list of Call Identifiers associated with a specific Incident Tracking Identifier. The request includes the <IncidentIdURN>. The response includes zero or more <CallIdURN>(s). A <MessageResult> is also returned that can include:

200 Okay No error

517 No such incidentIdentifier

504 Unspecified Error

#### 5.13.4.6 ListIncidentsByDateRange

Returns a list of Incident Tracking Identifiers occurring within a time/date range. The request includes a <StartDateTime> Timestamp and an <EndDateTime> Timestamp. A variety of times are logged against an Incident. This function returns an Incident if any logged time falls within the StartDateTime-EndDateTime. The response includes zero or more <IncidentIdURN>(s). A <MessageResult> is also returned that can include:

200 Okay No error

518 Bad Timestamp

520 EndTime occurs before StartTime

504 Unspecified Error

#### 5.13.4.7 ListIncidentsByLocation

Returns a list of Incidents that occurred within a specified geographic region. The request includes a GML shape in a <AreaOfInterestRequest> tag. A variety of locations are logged against an Incident. This function returns an Incident if any location logged against the Incident intersects any part of the areaOfInterest. The response includes zero or more <IncidentIdURN>(s). A <MessageResult> is also returned that can include:

200 Okay No error

521 Bad or missing Geoshape

504 Unspecified Error

#### 5.13.4.8 ListIncidentsByDateAndLocation

A combination of ListIncidentsbyDateRange and ListIncidentsByLocation, the request includes a <StartDateTime>, <EndDateTime> and <AreaOfInterestRequest>. The response includes zero or more <IncidentIdURN>(s). ). A <MessageResult> is also returned that can include:

200 Okay No error

519 Bad Timestamp

520 EndTime occurs before StartTime

521 Bad Geoshape

504 Unspecified Error

#### 5.13.4.9 ListCallsByDateRange

Returns a list of Call Identifiers occurring within a time/date range. The request includes a <StartDateTime> Timestamp and an <EndDateTime> Timestamp. The response includes zero or more <CallIdURN>(s). A <MessageResult> is also returned that can include:

200 Okay No error

519 Bad Timestamp

520 EndTime occurs before StartTime

504 Unspecified Error

#### 5.13.4.10 ListAgenciesByCallId

Returns a list of agencies involved in a call, including those referenced in AdditionalAgency events for the call. The request includes a <CallIdURN>. The response includes zero or more <AgencyId>(s). A <MessageResult> is also returned that can include:

200 Okay No error

516 No such callIdentifier

504 Unspecified Error

#### 5.13.4.11 ListAgenciesByIncidentId

Returns a list of agencies involved in an Incident, including those referenced in AdditionalAgency events for all calls associated with the Incident. The request includes an <IncidentIdURN>. The response includes zero or more <AgencyId>(s). A <MessageResult> is also returned that can include:

200 Okay No error

517 No such incidentIdentifier

504 Unspecified Error

### 5.13.5 Instant Recall Recorder

The ability to quickly review current or recent emergency communications content must be provided. The Logging Service's Web Service interface supports this capability with the query, retrieval and streaming media functions described in Section 5.13. 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 on which agents may access media.

### 5.13.6 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 interfaces identical to LogEvent (Section 5.13.3). 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 LogEventTimestamp in the header, 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.

### 5.13.7 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 it. Media are recorded as specified in Section 5.13, 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.

### 5.13.8 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.

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 log events 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.

## 5.14 Forest Guide

The ECRF and LVF infrastructure make use of Forest Guides as defined in RFC 5582 [60]. A server that does not answer a query can refer to a Forest Guide to determine the response.

### 5.14.1 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 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.

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.

### 5.14.2 Interface Description

The National Forest Guide maintains a LoST interface, as described in Section 4.4, for query resolution. It also maintains a LoST-sync interface defined in RFC 6739 [111] 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:nena:service:sos” and “urn:nena: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 5.3.5 and provides the same notification service described.

The Forest Guide must implement the server-side of the ElementState event notification package.

### 5.14.3 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.

### 5.14.4 Roles and Responsibilities

The Forest Guide must be managed nationally (agency not yet identified) and may evolve to an entity more representative of all public safety agencies. State ECRF and LVF operators are responsible to arrange for their coverage regions to be provisioned in the National Forest Guide. The National Forest Guide operator will maintain well-known contact information so that other National Forest Guides can arrange to exchange their coverage regions and mappings.

### 5.14.5 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.

### 5.14.6 Security Considerations

Since the National Forest Guide could be a bottleneck in the routing of emergency calls, it is an attractive attack target. For this reason, there are both internal and external National Forest Guides. The Internal Forest Guide is internal to the (national) ESInet and only allows queries from entities inside the ESInet. The external Forest Guide is public and allows queries from any source. When it is attacked, the Internal Forest Guide may refuse queries from any entity it does not have existing entries for (nominally state level ECRFs, and the National Forest Guides of other nations). 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 active attack, 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.

## 5.15 DNS

All elements identified by hostnames must have corresponding Domain Name Service (DNS) records as specified in STD13 [105] 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, and resolvers must be able to use cached records even if they have expired if they lose connections to authoritative DNS servers to resolve names. DNSSEC [155] 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 [106] 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 a domain name via U-NAPTR (RFC 4848 [193 [194]]), and U-NAPTR resolution may also be required to obtain the URI for a LIS (per RFC 5986).

## 5.16 Agency Locator

The ESInet will connect to many public safety agencies. A directory ("white pages" and "yellow pages") of agencies, together with key information about the agency, is the function of the Agency Locator. The Agency Locator is a distributed database. There are several mechanisms by which the agency locator can be searched to locate a specific agency. An agency is identified by an agency Identifier (See Section 3.1.1) and the agency identifier is the key that may be used to retrieve information from the Agency Locator about an agency.

One primary way to search the Agency Locator is by name. The Agency Locator provides a name (white page) search function, with wild cards, to find a specific agency. Another method to search is by location and agency type.

An Agency Locator Service is provided in the ESInet. Every Public Safety Agency connected to the ESInet is listed in the Agency Locator. The Agency Locator has two components:

a) An Agency Locator Record Store (ALRS) which holds the actual data record for the agency;

b) A search component, which uses the ECRF and a LoST query to find a given agency by type and location.

An agency locator record is identified by a URI whose domain is an ALRS. The URI can be presented to an ALRS that will respond with the record. The ECRF returns the URI.

Each FE in the Agency Locator must implement the server-side of the ElementState event notification package. The Agency Locator FE must promptly report changes in its state to its subscribed elements.

The set of Agency Locator FEs within an ESInet must implement the server-side of the ServiceState event notification package for the Agency Locator. Since the Agency Locator Service is typically a state-wide service it is recommended that the state level Agency Locator subscribe to ElementState for each Agency Locator FE within the state and provide a single Agency Locator ServiceState notifier for the entire state.

### 5.16.1 Agency Locator Record Store

An Agency Locator Record Store is a web service that, when presented with an agency locator URI, returns the agency locator record. The ALRS uses a simple HTTPS GET with the URI. The querier must use his credentials to create the TLS connection, and the credential and its corresponding agency type and role may influence what information is returned.

The ALRS may be operated by the agency itself, the ESInet operator may operate an ALRS for the entire ESInet, or any other party may operate an ALRS. Every agency must have a record stored in at least one ALRS, with the URI for that record stored in the ECRF that serves the agency.

### 5.16.2 Agency Locator Search by Location

The ECRF is used for an Agency Locator search function. For this purpose the service URNs for all agency types are defined, starting with "urn:nena:service:agencyLocator". For example, to find the agency locator record for the police department that serves the city of Wonderville, IA, an ECRF query with a PIDF with country US, A1=IA, A3=Wonderville and service URN of "urn:nena:service:agencyLocator.police" is performed. The ECRF would return a URI pointing to an ALRS that would return the agency locator record for the Wonderville police department when presented with the URI. The ECRF would return more than one URI if there was more than one police agency that served parts of Wonderville known to the ECRF resolving the query[44]. Since the URN for the search is in the "urn:nena:service" tree, the National Forest Guide provides a referral service allowing any agency on any ESInet to locate the ALRS for any location anywhere when searched by location.

The service URNs that are used for this function are defined in a registry, see Section 11.21.

### 5.16.3 Agency Locator Search by Name

A search for an agency where the search key is a name is provided by the Agency Locator Search Service. The Service is operated by the ESInet operator. The search function may return one or more Agency Locator URIs, a referral to another Agency Locator Search Service, or an error.

**ALSBNRequest**

| Parameter | Condition | Description |
|---|---|---|
| name | Mandatory | Name, or part of a name |

**ALSBNResponse**

| Parameter | Condition | Description |
|---|---|---|
| agencyLocatorRecordURI | Conditional, provided unless an error occurred | URI of an AgencyLocator Record or another Search Service. May occur more than once |
| statusCode | Mandatory | Status Code |

Status Codes

200 Okay No error

303 Iterative Refer (Contains referral URI)

[44] The fact that the response may not include all agencies serving the area in the query is a limitation of the LoST protocol. Future changes in LoST, or workarounds in this document will be necessary to allow a query like this example to identify all the appropriate agencies.

526 No Data Found

504 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 revision of this document will specify a more general way to connect the Agency Locator Search Services.

### 5.16.4 Agency Locator Record

The data returned by dereferencing an agency locator record URI is an xml data structure containing the following elements:

| Element Name | Type (note 1) | Condition | # Occ | Use |
|---|---|---|---|---|
| agencyXcard | xCard | M | 1 | Agency Contact information |
| type | Responder name[45] | M | 1-n | Agency Type (psap, police, fire, …) |
| emergencySipInterface | URI | C Note 1 | 1 | Interface where 9-1-1 SIP calls are accepted (Note 2) |
| adminLine | URI | C Note 3 | 1 | sip or tel: URI containing 10 digit admin line #, see Section 5.2.1.1. |
| logger | URI | C Note 4 | 1-n | Agency Logger interface, see Section 5.13.1 |
| EIDDinterface | URI | C Note 5 | 1 | EIDD Interface URI, See section 5.13.1 |
| SvcState | URI | R | 1 | Service State Subscription URI |
| DscRptSvc | URI | C Note 6 | 1 | Discrepancy Report Service URI, see Section 4.7 |
| headXcard | xCard | O | 1 | xCard of top agency official |
| onDutySuperXcard | xCard | O | 1 | xCard of supervisor on duty now |

Note 1: For all URIs, if the agency provides the service, 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.

[45] Name from the responder type registry defined in Section 11.4

Note 2: This URI must be the same URI obtained from the SRV record for the SIP service for the domain of the 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.

Note 4: Although unusual, not all agencies have a logger.

Note 5: Although unusual, not all agencies have an EIDD interface.

Note 6: Although unusual, not all agencies have a Discrepancy Reporting Service.

## 5.17 Policy Store

### 5.17.1 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.

### 5.17.2 Interface Description

A Policy Store implements the policy storage and retrieval functions defined in Section 4.3.1. 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.

### 5.17.3 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.

## 5.18 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.

## 5.19 Origination Networks and Devices

A device, network or service provider presenting calls to an ESInet is expected to support the following interfaces. How the origination network, device or service arranges its emergency calling services to meet this standard is beyond the scope of this document.

### 5.19.1 SIP Call Interface

The origination network is expected to present calls to the ESInet meeting the ESInet SIP interface specified in Section 4.1. All calls will be signaled with SIP, must contain a Geolocation header, 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.

### 5.19.2 Location by Reference

Origination networks that are also access networks are expected to also provide a Location Information Server function (that is, location dereference, and location validation if applicable) meeting the requirements of Section 5.10, if they supply location by reference.

### 5.19.3 Additional Data Repository

Origination networks and devices presenting calls to ESInets are expected to provide an Additional Data Repository interface meeting the requirements of Section 5.11 unless they always send Additional Data by value.

## 5.20 Map Database Service

The Map Database Service is used to provide a PSAP handling a call out of area with the information needed to show a call taker a map of the vicinity where the caller is located. The Map Database Service is queried with the location and boundaries to be covered and returns a set of map features and/or imagery covering it to be displayed.

Note: The details of the Map Database Service and its interfaces will be provided in a future revision of this document.

# 6 Security

## 6.1 Identity

Each agency and each agent in an agency are issued credentials that allow them to be identified to all services in the ESInet[46]. An agency identifier is a globally unique domain name (such as "erie.psap.ny.us"), which appears in the SubjectAltName of an X.509 [181] 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 domain name 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 3.1.

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.

[46] Even though an ESInet may be engineered with IPsec paths that do not need agent credentials to create secure paths, handling calls out of area or in situations where pre-provisioned paths fail would require agents having credentials.

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.

Operating a CA requires the creation of, and strict adherence to a Certificate Policy and Practice Statement (CP/CPS). 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.

The identities, and the credentials, must be presented to gain access to ALL services and data in the ESInet.

## 6.2 PSAP Credentialing Agency

NENA will facilitate the creation of or operate the PCA. The PCA CP/CPS must be in conformance with the minimum standards to be provided in a future revision of this document. Any agency or agent may obtain a certificate from the PCA directly. As this is a similar function to the Valid Emergency Services Authority (VESA) in i2, it is expected that the VESA and the PCA are the same entity. Prior to the PCA being available, NG9-1-1 implementations should accept credentials issued by any certificate authority listed in the current Firefox browser[47].

## 6.3 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 – the entity responsible for alerting and directing the response of public safety responders to the desired location.
- 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.

[47] See https://wiki.mozilla.org/CA:IncludedCAs

- 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:nena:service:responder" Registry (see Section 11.4).

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

This document creates a new registry to be managed by NRS for Agency Roles. See Section 11.18. 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.
- 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, 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
- Assist 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 revision of this document. This document creates a registry of Agent Roles to be managed by NRS. See Section 11.19.

## 6.4 Authentication

Authentication of Agents accessing elements described in this document must be implemented with a universal Single Sign On paradigm. The mechanism used is OASIS SAML (Security Assertion Markup Language). There are two entities: an Identity Provider (IDP) which authenticates users and supplies services 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 an operation should be permitted by the user. Agents in PSAPs and Responder Agencies, as well as other service agencies with agents use the Single Sign On 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 to establish the TLS session.

For applications that depend upon interactions with Agents, several profiles of the Security Assertion Markup Language version 2 [84] 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 [84], transport bindings [164], and a set of concrete profiles [165], 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 [166] 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 [165]:

- 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 SAML2 assertions, in the presence of a web browser based user-agent, which is used as the 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 [165] 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 that the client is capable of authenticating to. It is recommended that this be the primary means for IDP discovery for an actor. Providers are identified by a URI as defined above.

### 6.4.1 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 [166], 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 are 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) [196]
- Biometrics, including fingerprints, palm prints, retina scans, face 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 where the authentication server and enrollment server use the same brand of scanner. Further if network access to the authentication data is 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-1024 (see RFC 3447 [197]) with the credentials rooted in the PCA, typically over TLS or IPsec. All elements in the ESInet must accept RSA-1024 with a certificate rooted in the PCA. They may accept alternate authentication cryptosystems as long as they are at least as strong as RSA-1024. RSA-1024 must be supported by all implementations.

All protocol exchanges across the ESInet should be authenticated.

## 6.5 Authorization and Data Rights Management

Authorization and Data Rights Management in NG9-1-1 is based on XACML 1.0 [87]. 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.

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 role registry) 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 11.29 separated by an ampersand, data items are named by the xml namespace 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 “urn:ietf:params:xml:ns:pidf:geopriv10: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.

## 6.6 Integrity Protection

All protocol operations must be integrity-protected (via TLS or IPsec), using SHA-256 [198]. Alternate integrity protection algorithms are acceptable as long as they are at least as strong as SHA-256 as long as both sides can implement it. SHA-256 must be supported by all implementations. Implementations must implement TLS. IPsec may be used between two elements instead of TLS, but the inability to determine the role or identity of the client of a server, or the server to a client prohibits use of many of the security mechanisms described above.

### 6.7 Privacy

All protocol operations must be privacy protected via TLS (or IPsec as applicable), preferably using Advanced Encryption Standard (AES). Systems currently using Data Encryption Standard (DES) or triple DES must be upgraded to at least AES. 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 or an equivalently strong algorithm. Access to encryption keys must be defined by a management policy that is strictly adhered to. Keys must never 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 [147] 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 must be supported by all implementations.

### 6.8 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) 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 revision of this document could change the mandatory algorithm requirements. IPsec may be used between two elements instead of TLS, but the inability to determine the role or identity of the client of a server, or the server to a client prohibits use of many of the security mechanisms described above.

## 7 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 7-1. The following subsections 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 [151].

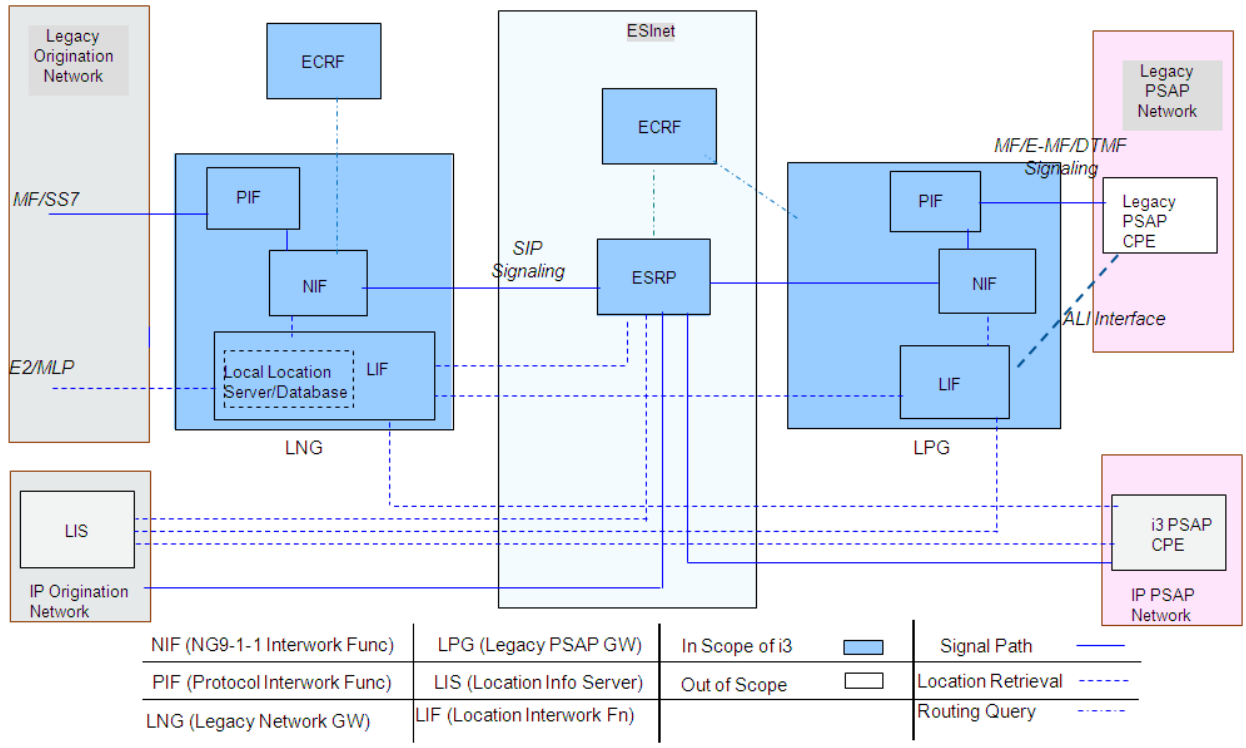



**Figure 7-1 i3 Gateways - Functional Architecture**

## 7.1 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.

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 7-1.[48] 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 [116]. It is assumed that the PIF functional component does not require specialized hardware, and can therefore be implemented using commercially available hardware. (See Section 7.1.1 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 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 7.1.2 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[49]. 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 7.1.3 for further details.)

[48] 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.

[49] 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 dispatch location associated with the emergency call.

Where 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 5.13.3 of this document.

### 7.1.1 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.

#### 7.1.1.1 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:

- 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 7.1.1.1.

#### 7.1.1.2 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.

##### 7.1.1.2.1 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)[50]. 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

[50] 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.

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.
- 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 [180], Chapter T1.110.1, Section 5.1 and Chapter T1.111.3, Section 2.

#### 7.1.1.2.2 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 [199], *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 [200], 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 will also generate a SIP BYE message toward the NIF, as described in Section 7.1.1.5.

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.

### 7.1.1.3 Early Media

In order to provide the equivalent of "trunk-side recording", an LNG is expected provide Early Media [37] 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 [154] SRC (Session Recording Client) shall provide Early Media [37] to the SRS (Session Recording Server).

#### 7.1.1.4 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 [117] real time text. Likewise, the PIF component will be responsible for generating Baudot tones in outgoing media if real-time text is received in RTP packets.

To support TTY calls, the PIF component will include an SDP in the INVITE message sent to the NIF component that describes a media format associated with real time text, as described in RFC 4103.

#### 7.1.1.5 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 [167]**,** 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 SIP INVITE generated by the PIF will 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 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 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 will be populated with the information signaled in the SS7 Calling Party Number parameter (if present**).**
- A P-Asserted-Identity (P-A-I) header 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 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 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 that contains the trunk group parameters that identify the ingress trunk group to the Legacy Network Gateway, as defined in RFC 4904 [201].
- A Via header that is populated with the element identifier (see Section 3.1.3) for the Legacy Network Gateway.
- An SDP offer that includes the G.711 codec. To support incoming TTY calls, the SDP offer will describe a media format associated with real time text as described in RFC 4103 [117].

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.

The PIF component of the Legacy Network Gateway shall also be capable of receiving and processing a 180 Ringing message. 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 [167] 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 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-317-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 SIP message received), the Legacy Network Gateway will 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 will 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.

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.

If the PIF component receives other SIP messages from the NIF component, it shall process them per RFC 3261 [12].

### 7.1.2 NG9-1-1 specific Interwork Function (NIF)

#### 7.1.2.1 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 will 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 will make this determination based on the incoming trunk group parameters included in the Contact header of the INVITE message from the PIF. If the call is received over an SS7 trunk group, the NIF will make this determination based on the coding of the cpc and oli parameters in the P-A-I header of the INVITE message from the PIF and/or the ingress trunk group parameters in the Contact header of the INVITE message from the PIF. Based on this determination, the NIF will 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 7.1.3 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 headers of the INVITE message received from the PIF contains the same CPN/ANI), the NIF will pass this number to the LIF to use in retrieving the location for the call[51]. 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 and a different URI associated with the CPN in the P-A-I header) 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 or the trunk group information in the Contact header) 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 will 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 of the received INVITE, where to extract the callback information and ESRD from. The ESRD may be populated in the Request URI/To headers or in the "From" header. The MDN may be populated in the "From" header or the P-A-I header.

(See Section 7.1.3 for further discussion of what the LIF does with this information.)

#### 7.1.2.2 NIF Handling of Location Information from the LIF

Once the NIF receives location information from the LIF in geo or civic format, the NIF must be capable of generating a routing request to an ECRF. The NIF shall generate a LoST query, which

[51] 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.



One Nation 9-1-1 One Number

includes the location information provided by the LIF and an appropriate service URN (i.e., "urn:service:sos"), following the procedures described in Section 4.4. 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 of the INVITE message from the PIF component) to query the ECRF.

Upon receiving the response from the ECRF, the NIF will 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.

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 [104], as well as any other non-location information associated with the call that is provided to the NIF by the LIF, formatted according to [143]. 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 will contain the URI of the ADR where 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, it will include the reference URI in the Call-Info header field of the INVITE message sent to the ESRP, with a purpose parameter beginning with "EmergencyCallData". 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 [202], to support dereference requests for Additional Data.

#### 7.1.2.3 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 INVITE message will contain information received in the INVITE message from the PIF component, as well as location and possibly callback information received from the LIF component. The INVITE message may also contain a reference URI associated with the Additional Data structure generated by the NIF, if one is generated. Specifically, the INVITE message will contain the following information:

- A Request-URI that contains a service URN in the "sos" tree (i.e., "urn:service:sos")
- A To header that contains the digits "911"
- A "From" header that contains the callback number (or Originating TN for legacy wireline emergency call origination**s)** received by the NIF component in incoming 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 will populate the "From" header based on the

Calling Party Number received in the "From" and P-A-I headers 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 will populate the "From" header as follows:
  - If the "From" header and the P-A-I header 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 of the INVITE message from the PIF component to populate the "From" header of the outgoing INVITE message.
  - If the "From" header and the P-A-I header 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 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 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 will contain a value of "Anonymous."

- A P-Asserted-Identity (P-A-I) header 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 will populate the P-A-I with the SS7 Calling Party Number information received in the P-A-I header 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 will populate the P-A-I header as follows:
    - If the "From" header and the P-A-I header 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 of the INVITE message from the PIF component to populate the P-A-I header of the outgoing INVITE message.
    - If the "From" header and the P-A-I header 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 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 from the outgoing INVITE message.

  - If a non-initialized mobile caller originated the call, the P-A-I header will be omitted.

- A P-Charge-Info header, 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 that is populated with the element identifier (see Section 3.1.3) for the Legacy Network Gateway
- A Route header that contains the ESRP URI obtained from the ECRF
- A Contact header that contains a SIP URI that is associated with the Legacy Network Gateway
- A Supported header that contains the "geolocation" option tag
- A Geolocation header that either:
  - Points to the message body (using a "Content Identifier" URI, as defined in RFC 2392 [169]) where a PIDF-LO containing the location value retrieved by the LIF is coded (see Section 7.1.3 and [10])[52]
  - Contains a location-by-reference URI[53]
- A Geolocation-Routing header 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[54] Call-Info header fields with a purpose parameter beginning with "EmergencyCallData" and a URI associated with the ADR that contains the Additional Data data structure which, when dereferenced, would yield additional information about the call.
- If, during the processing of the emergency call, the NIF component of the Legacy Network Gateway creates two 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 the data structures in the body of the INVITE message and shall include one or more

[52] This method will be used for wireline emergency calls.
[53] This method will be used for wireless Phase 1 and Phase 2 calls to allow the queries for routing location as well as for initial and updated dispatch location.
[54] The NIF must add at least ProviderInfo and ServiceInfo and may add SubscriberInfo blocks as described in Section 5.11. These may be referenced in one Call-Info header field with multiple URIs or multiple Call-Info header fields with one or more URIs.

Call-Info header fields having a purpose parameter prefix of "EmergencyCallData" that contain a cid: URI that points to the information in the message body.

- A P-Preferred-Identity header 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 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 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 will reference the existing dialog so that the i3 PSAP (or Legacy PSAP Gateway, 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 will include the following information:

- A Request-URI that contains the information provided in the Contact header of the 200 OK message that was returned in response to the original INVITE message
- A To header that contains the same information as the original INVITE message (i.e., the digits "911")
- A "From" header that contains the same information as in the original INVITE message (i.e., the "From" header 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 that contains the callback number retrieved by the LIF component
- A Via header that is populated with the element identifier (see Section 3.1.3) for the Legacy Network Gateway
- A Route header that contains the same information as in the original INVITE (i.e., the ESRP URI obtained from the ECRF)
- A Contact header that contains the same information as in the original INVITE message (i.e., a SIP URI associated with the Legacy Network Gateway).

The i3 PSAP/Legacy PSAP Gateway will return a 200 OK to indicate that it accepts the change, and the Legacy Network Gateway will respond to the 200 OK by returning an ACK message.

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.

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 [12]. 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.

### 7.1.3 Location Interwork Function (LIF)

At the request of the NIF, the LIF will 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 will 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 will be used for both routing and dispatch purposes.
- If the call is a Phase I wireless emergency call for which static dispatch 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 will use the locally stored information as the dispatch location for the call**.**
- 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 dispatch location information.

The data in the internal location server/database may be provisioned using proprietary mechanisms/interfaces (e.g., using the existing provisioning flows, systems and interfaces that are used for provisioning legacy ALI databases today), or using a standard provisioning interface, as specified in a subsequent NENA standard, or some combination thereof, depending on the business agreements that exist between the Legacy Network Gateway provider and the data owners.

The LIF may receive one or two numbers/keys[55] from the NIF to be used for location retrieval/acquisition. Upon receiving the key(s), the LIF will 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 will utilize internally defined procedures/protocols to retrieve static location information which will 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 will 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. Dispatch 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 will 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 or MLP query (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 dispatch 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-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 required Additional Data XML documents.

If the call originated in a legacy wireless network using Wireline Compatibility Mode, the LIF will interrogate its steering data with the ESRK. The steering data will contain the address of the MPC/GMLC in the legacy wireless network that should be queried for initial/updated dispatch location. The LIF component will 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 dispatch location, containing the ESRK, to the MPC/GMLC and must be capable of processing an E2/MLP response. The LIF component will 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 dispatch location returned by the MPC/GMLC (which is initially expected to convey information about the location of the cell site/sector), the LIF

[55] 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 is not required to truncate if the origination network can present more than 10 digits.

component shall store the dispatch 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 will 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 dispatch 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 dispatch location. The LIF will 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 will 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 will 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 dispatch location.
- If the LIF component finds steering data corresponding to the ESRD, it will obtain the routing location for the call by consulting an associated database that contains static mappings of ESRD to routing location chosen so that it will route to the target PSAP associated with the ESRD. The LIF component will also generate an E2/MLP query for dispatch location, containing the callback number and ESRD, to the MPC/GMLC and must be capable of processing an E2/MLP response. The LIF component will 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 will 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 dispatch 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 dispatch 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 4.2. 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.

#### 7.1.3.1 Interworking to Support Location Dereferencing

##### 7.1.3.1.1 Interworking Between HELD and E2

The following tables illustrate the interworking between HELD and E2 to support location dereferencing.

**Table 7-1 HELD locationRequest to E2 ESPOSREQ Mapping**

| HELD locationRequest→ | ESPOSREQ→ | Notes |
|---|---|---|
| locationURI | - | Reflects value provided in the Geolocation header of the INVITE message sent by the LNG |
| locationType | - | May include the optional "exact" attribute and indicates "civic" and/or "geo" |
| 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 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, 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 | |

| HELD locationRequest→ | ESPOSREQ→ | Notes |
|---|---|---|
| - | 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 |

**Table 7-2 E2 esposreq to HELD locationResponse Mapping**

| esposreq→ | HELD locationResponse→ | Notes |
|---|---|---|
| - | presence | Contains civic and/or geo 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 |

| **esposreq→** | **HELD locationResponse→** | **Notes** |
|---|---|---|
| Position Information:<br>- Generalized Time<br><br>- Geographic Position<br><br><br><br><br>- Position Source | presence | <br>Indicates time of position determination<br><br>One or the other of Position Information – Geographic Position or Location Description may be populated**, and when present,** must be populated with geo location and civic address, respectively. Both may be populated if both are available at the MPC. Geographic Position would map to geo location formatted as a PIDF-LO<br><br>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 |

| 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. |

#### 7.1.3.1.2 Interworking Between HELD and MLP

The following tables illustrate the interworking between HELD and MLP to support location dereferencing.

**Table 7-3 HELD locationRequest to MLP ELIR Mapping**

| HELD locationRequest→ | MLP ELIR→ | Notes |
|---|---|---|
| locationURI | - | Reflects value provided in the Geolocation header of the INVITE message sent by the LNG |
| locationType | - | May include the optional “exact” attribute and indicates “civic” and/or “geo” |
| 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, the LNG shall return the most accurate location it has locally (e.g., Phase I or Phase II). |

| HELD locationRequest→ | MLP ELIR→ | Notes |
|---|---|---|
| - | Header:<br>- hdr ver=" 3.2.0"<br>- client<br>○ id<br>○ pwd<br>○ service id | 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 | |
| - | EQOD<br>- 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 7-4 MLP ELIA to HELD locationResponse Mapping**

| MLP ELIA→ | HELD locationResponse→ | Notes |
|---|---|---|
| - | presence | Contains civic and/or geo 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 |

| MLP ELIA→ | HELD locationResponse→ | Notes |
|---|---|---|
| EME_POS | | |
| - MSID | - | From the ELIR message |
| - ESRD | | From the ELIR message |
| - Position Data | | |
| ○ Time | presence | 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 |
| pos_method[3] | | 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" |
| | | 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 parameter is not provided in Canadian networks today.

#### 7.1.3.1.3 Interworking Between SIP Presence and E2

Using SIP Presence with location by reference is discussed in Section 5.10. The following tables illustrate the interworking between SIP Presence and E2 to support location dereferencing.

**Table 7-5 SIP Presence SUBSCRIBE to E2 ESPOSREQ Mapping**

| SIP Subscribe→ | ESPOSREQ→ | Notes |
|---|---|---|
| location URI (in RequestURI and To:) | - | Reflects value provided in the Geolocation header of the INVITE message sent by the LNG |

| SIP Subscribe→ | ESPOSREQ→ | Notes |
|---|---|---|
| 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 |

**Table 7-6 E2 esposreq to SIP Presence NOTIFY Mapping**

| esposreq→ | SIP NOTIFY→ | Notes |
|---|---|---|

| esposreq→ | SIP NOTIFY→ | Notes |
|---|---|---|
| - | presence | Contains civic and/or geo 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:<br>- Generalized Time<br>- Geographic Position<br>- Position Source | presence | Indicates time of position determination<br>One or the other of Position Information – Geographic Position or Location Description may be populated**, and when present,** must be populated with geo location and civic address, respectively. Both may be populated if both are available at the MPC. Geographic Position would map to geo location formatted as a PIDF-LO<br>Method of location determination; Position Source maps to 'Method' parameter within PIDF-LO |
| Callback Number - Response | - | Populated with MDN/MSISDN that identifies the caller |

| esposreq→ | SIP NOTIFY→ | Notes |
|---|---|---|
| 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 |
| 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 Afor mappings of data elements received in Location Description Parameter to the PIDF-LO or Additional Data structure. |

#### 7.1.3.1.4 Interworking Between SIP Presence and MLP

The following tables illustrate the interworking between SIP Presence and MLP to support location dereferencing.

**Table 7-7 SIP Presence SUBSCRIBE to MLP ELIR Mapping**

| SIP SUBSCRIBE→ | MLP ELIR→ | Notes |
|---|---|---|
| location URI (in RequestURI and To:) | - | Reflects value provided in the Geolocation header 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. |

| SIP SUBSCRIBE→ | MLP ELIR→ | Notes |
|---|---|---|
| - | Header:<br>- hdr ver=" 3.2.0"<br>- client<br>o id<br>o pwd<br>o service id | 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 | |
| - | EQOD<br>- 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 7-8 MLP ELIA to SIP Presence NOTIFY Mapping**

| MLP ELIA→ | SIP NOTIFY→ | Notes |
|---|---|---|
| - | presence | Contains civic and/or geo location populated in a PIDF-LO; If this is the first NOTIFY, 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 |

| MLP ELIA→ | SIP NOTIFY→ | Notes |
|---|---|---|
| EME_POS | | |
| - MSID | - | From the ELIR message |
| - ESRD | | From the ELIR message |
| - Position Data | | |
| ○ Time | presence | 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 |
| pos_method[3] | | This geo-location will be formatted as a PIDF-LO for population in the NOTIFY if this is not the first one. |
| | | 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 parameter is not provided in Canadian networks today.

#### 7.1.3.2 Call Flow Example

Figure 7-2 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.

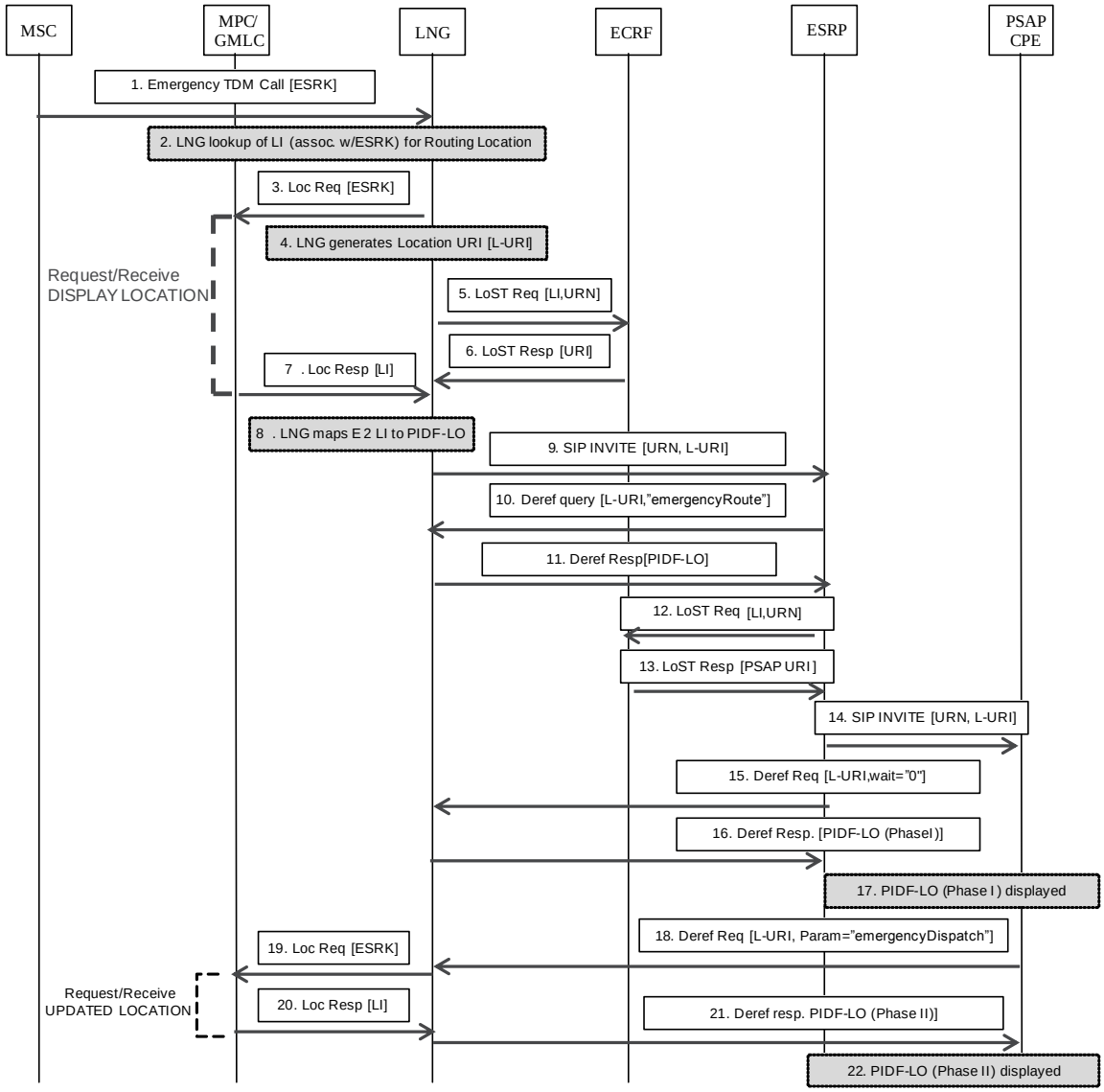



**Figure 7-2 Example Call Flow**

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.
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.
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).
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.

## 7.2 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 [203]) on the other. The Legacy PSAP Gateway also includes an ALI interface (as defined in NENA 04-001 [204] or NENA 04-005 [205]) 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 7.2.2 for further discussion.

The Legacy PSAP Gateway functional element contains three functional components, as illustrated in Figure 7-1[56]:

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 protocols, as appropriate for the interconnected PSAP[57]. 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 [116]. The PIF component must also be capable of interworking text messages received in an MSRP session with TTY[58]. It is assumed that the PIF functional component does not require specialized hardware, and can therefore be implemented using commercially available hardware. (See Section 7.2.1 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,

[56] 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.

[57] 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.

[58] Details describing the interworking of text messages received via an MSRP session with TTY will be provided in a future issue of this specification.

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 7.2.2 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 7.2.3 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 5.13.3 of this document.

### 7.2.1 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 [179].

The PIF component of the Legacy PSAP Gateway must be capable of accepting a SIP INVITE message generated by the NIF component (see Section 7.2.2.3).

Upon receiving the INVITE method, the PIF component of the Legacy PSAP Gateway will 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 will 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[59]. (See Section 7.2.3 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

[59] The "ANI" may contain the caller's callback information or a query key (i.e., a pANI).

and "Special Handling" indication. The traditional MF and E-MF signaling interfaces that may be supported by a legacy PSAP are described below.

#### 7.2.1.1 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:

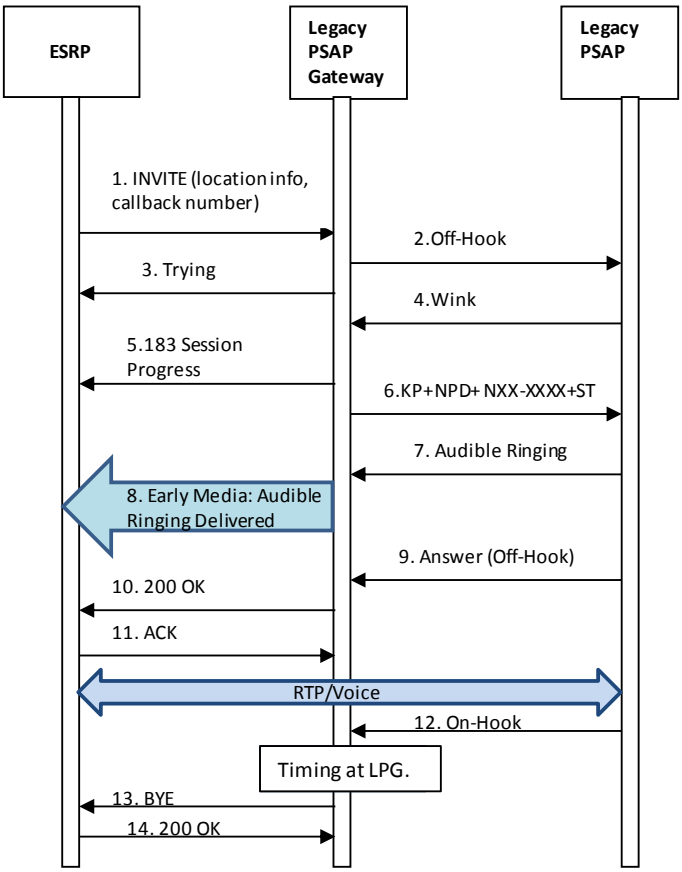



**Figure 7-3** Call Delivery with Traditional MF Interface to PSAP

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. 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 [12], with the clarifications provided in Sections 4.1 and 7.2.2.
2. When the NIF component of the Legacy PSAP Gateway receives the INVITE message, it follows the procedures described in RFC 3261 [12] 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 Numbering Plan Digit [NPD][60] 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 will 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 of the incoming INVITE message.

If the P-A-I or the "From" header 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 will identify an NPD associated with the NPA and will signal the NPD-NXX-XXXX in the "From" header of the INVITE message sent to the PIF component. The PIF component will 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 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 will identify an NPD associated with an NPA that is appropriate for the target PSAP, and will 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[61].

The NIF will signal the pANI in the "From" header of the INVITE message it sends to the PIF.

If, based on provisioning, the PSAP should only receive a location key, the NIF will signal that information to the PIF in a "From" header 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).

[60] See Section 7.2.2.2 for further discussion of NPD digits.

[61] 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.

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[62], 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 will signal the SIP 500 Server Internal Error message back to the ESRP. (See Section 7.2.4.1 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.

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 ends with the Start (ST) signal. (See GR-350-CORE or NENA 04-001 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 (500 +/- 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

[62] The 4-second timer is specified in ATIS 0600414.1998(2007), *Network to Customer Installation Interfaces – Enhanced 911 Analog Voicegrade PSAP Access Using Loop Reverse-Battery Signaling*.

that this interval be a minimum of 1100ms. See Section 7.2.4.2 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.

#### 7.2.1.2 Enhanced MF (E-MF) Interface

As described in Section 7.2.2.3, 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',**

where NPA NXX XXXX is the Calling Station Number obtained from the "From" header 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 of the INVITE message from the NIF. (See Section 7.2.2.2 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.

Where 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 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 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 of the INVITE message from the NIF. (See Section 7.2.2.2 for further discussion of the encoding of the II digits.)[63] Today, this scenario is typically associated with the delivery of wireless emergency calls to legacy PSAPs.

With respect to legacy emergency call originations, 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, if the PSAP is only capable of receiving one 10-digit number, and both callback information and location

[63] See GR-2953-CORE or NENA 03-002 for further discussion of MF signaling sequences associated with E-MF interfaces.

information are received by the Legacy PSAP Gateway in the incoming INVITE, the NIF component of the Legacy PSAP Gateway will 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 of the incoming INVITE message from the NIF. The II value to signal forward will be determined based on the information in the oli parameter in the "From" header of the received INVITE message.

(See Section 7.2.2.2 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 depicted in Figure 7-2for 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 7.2.2.3.1). 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 containing callback information and a "From" header 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 to populate the second MF sequence.

  The PIF will populate the II digits based on the oli parameter in the P-A-I header 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 of the INVITE message it sends to the PIF. The PIF will take the information from the "From" header 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 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 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 and a P-A-I header in the INVITE message from the NIF, it shall populate the first MF sequence based on the content of the P-A-I header, and the second MF sequence based on the content of the "From" header.

  If the PIF receives a "From" header and no P-A-I header in the INVITE message from the NIF, it will populate the II digits based on the oli parameter in the "From" header. If the PIF receives both a "From" header and a P-A-I header in the INVITE message from the NIF, it will populate the II digits based on the oli parameter in the P-A-I header.

#### 7.2.1.3 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 will be responsible for recognizing the Baudot tones in incoming media and replacing them with RFC 4103 [117] real time text.

#### 7.2.1.4 Handling of Media Associated with SMS, Instant Messaging and RTT

Interworking of SMS to MSRP is expected to occur outside the ESInet, but legacy PSAPs must have the capability to accept text messages. Interworking between MSRP and TTY must occur within the LPG. Specification for interwork between MSRP and TTY will be covered in a future revision of this document.

The PIF must interwork the RFC 4103 real time text generated by the NIF to Baudot tones.

#### 7.2.1.5 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.

### 7.2.2 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 4.1. 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
- Route header = PSAP URI resolving at the gateway[64]
- From = Callback Number/Address or "Anonymous," if unavailable

[64] 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" and the PSAP URI for PSAP "B" might be "psapB@gateway1.esinet.net". The domain of the gateway in this example would be "gateway1.esinet.net".

- 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)
- 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 headers present in the INVITE message received by the terminating ESRP)
- Contact = as received by the terminating ESRP (i.e., a SIP URI or tel URI identifying the user to facilitate an immediate call back to the device that placed the emergency call, or a SIP URI associated with a Legacy Network Gateway)
- 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 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 4244, with a Reason Parameter (will be present if call has undergone diversion).

Upon receiving an INVITE message from an ESRP, the NIF component will 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.

#### 7.2.2.1 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 where 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 will 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 7.2.1.1 and 7.2.1.2, the locally significant digit string delivered to the PSAP will be of the form "NPD/NPA-511-XXXX". If a pANI of the form 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 a NANP number.

#### 7.2.2.2 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 on 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 where a PSAP supports the delivery of a single 10-digit number over an E-MF interface and 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[65]. The ESRP shall use the History-Info header (RFC 4244 [44]) and the associated Reason parameter to communicate an indication of alternate/default routing. The NIF component of the Legacy Network Gateway will determine the appropriate coding of the NPD or II based on the content of received History-Info and Reason headers and provisioning associated with the destination PSAP.

#### 7.2.2.3 Internal Interface to the PIF Component

The NIF component will generate an INVITE message to be sent to the PIF component. This message will 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 will obtain callback information from the incoming INVITE message in the following way. If the incoming INVITE message contains a P-A-I header, it will use the information in this header as callback information. If the incoming INVITE message does not contain a P-A-I header, the NIF will look in the "From" header. If the "From" header contains a value other than "Anonymous", the NIF will use the content of the "From" header as the callback information. If the "From" header contains the value "Anonymous" and a P-Preferred-Identity header 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 of the incoming INVITE message.

If the PSAP supports a traditional MF interface, then the NIF will determine, based on provisioning associated with the destination PSAP, whether to populate the "From" header of the INVITE message that it sends to the PIF with an NPD + 7-digit number that is 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. 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 "0-911-0TTT" shall be signaled in the "From" header. In a legacy environment, the "TTT" represents an end office identifier associated with the incoming trunk group to the SR. Further study is needed to determine what should be populated as the "TTT" value for calls originating from VoIP customers.

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 will determine, based on per-PSAP provisioning, whether callback information or location information should be populated in the "From" header 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

[65] 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.

in the "From" header. 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 "000-911-0TTT" shall be signaled in the "From" header.

If the legacy PSAP supports an E-MF interface and is capable of receiving two MF signaling sequences, the NIF will populate a 10-digit number that represents location in the "From" header and a 10-digit number that represents callback information in the P-A-I header 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 "000-911-0TTT" for the missing information in the P-A-I or "From" header. 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 "000-911-0TTT" for both the Calling Station Number and the location reference. Further study is needed to determine what should be populated as the 'TTT' value for calls originating from VoIP customers.

#### 7.2.2.3.1 INVITE Message Sent from NIF Component to PIF Component

The INVITE message sent by the NIF component to the PIF component will 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
- Max Forwards <70
- Record Route = ESRP URI
- From = See Table 7-9
- To = sip:911@vsp.com
- P-A-I = See Table 7-9
- 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 7-9 Population of "From" and P-A-I Headers in INVITE Message Sent to PIF**

| PSAP Interface Supported | Scenario | "From" Header Content | P-A-I Header Content |
|---|---|---|---|

| PSAP Interface Supported | Scenario | "From" Header Content | P-A-I Header 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<br>Non-initialized mobile caller | NPD-511-XXXX (associated with location information) | Not present |
| Traditional MF | Location information desired; only callback information available | 0-911-0TTT | Not present |
| Traditional MF | Neither callback nor location available | 0-911-0TTT | Not present |
| 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)<br>oli parameter |
| Enhanced MF | Interface supports delivery of 20 digits; callback is available, location is not available | 000-911-0TTT | NPA-NXX-XXXX or NPA-511-XXXX (associated with callback information)<br>oli parameter |
| Enhanced MF | Interface supports delivery of 20 digits; location is available, callback is not available | NPA-511-XXXX (associated with location information) | 000-911-0TTT |
| 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"<br>oli parameter |

| PSAP Interface Supported | Scenario | "From" Header Content | P-A-I Header Content |
|---|---|---|---|
| Enhanced MF | Interface supports delivery of 20 digits; neither location nor callback is available | 000-911-0TTT | 000-911-0TTT |
| Enhanced MF | Interface supports delivery of 10 digits; Callback information expected and available | NPA-NXX-XXXX or NPA-511-XXXX (associated with callback information)<br>oli parameter | Not present |
| Enhanced MF | Interface supports delivery of 10 digits; Location information expected and available | NPD-511-XXXX (associated with location information)<br>oli parameter | Not present |
| Enhanced MF | Interface supports delivery of 10 digits; Callback information desired; only location information available | NPD-511-XXXX (associated with location information)<br>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)<br>oli parameter | Not present |
| Enhanced MF | Interface supports delivery of 10 digits; Neither callback nor location available | 000-911-0TTT | 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"<br>oli parameter | Not present |

#### 7.2.2.4 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 destination (e.g., using a speed calling feature), or by manually dialing the number of the desired 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 [66]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. The NIF will then generate a SIP REFER method to request that the caller (or B2BUA, depending on the architecture being used by the ESInet to support call transfer) be invited to the conference. 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. 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 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 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 of the outgoing REFER method

[66] 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.

- 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.[67] The NIF will then use the URI returned in the response from the ECRF to populate the Refer-To header of the outgoing REFER method.[68]

Figure 7-4 and Figure 7-4 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 7-3 shows the establishment of a conference by the Legacy PSAP Gateway in response to a transfer request from a legacy PSAP. Figure 7-5 shows the completion of the transfer of the emergency call to the secondary PSAP. Section 4.1.1.2 provides a more complete discussion of the REFER method, and Sections 5.8 and 5.9 provide detail flows describing the alternatives for supporting bridging and transfer in an i3 environment.

[67] 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.

[68] 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.



One Nation 9-1-1 One Number

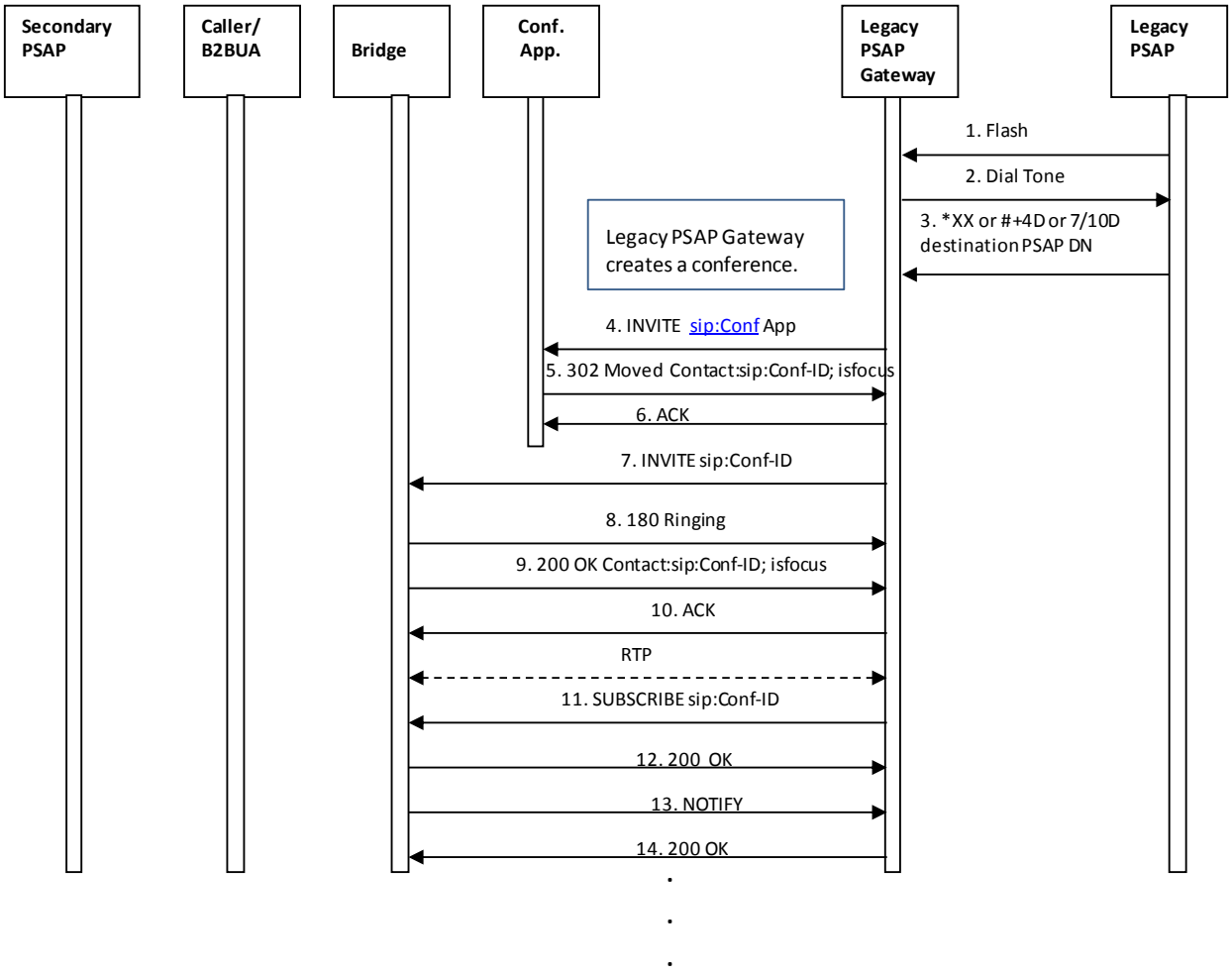



**Figure 7-4 Emergency Call Transfer Request from Legacy PSAP – Conference Established**

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. – 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 Section 5.8. 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 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. The Legacy PSAP Gateway will populate the remaining fields of the REFER based on RFC 3515.

As described in Section 5.8, the Legacy PSAP Gateway shall be capable of receiving a 202 Accepted 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 secondary PSAP is answered, the Legacy PSAP Gateway will receive a NOTIFY message indicating this event. The Legacy PSAP Gateway will respond to the NOTIFY by returning a 200 OK message.

The Legacy PSAP Gateway will create an Emergency Incident Data Document (EIDD) that contains location information (by value or reference), the Additional Data blocks, as well as any Additional Data structures if received by the Legacy PSAP Gateway with the call, and will pass this information to the secondary PSAP, as described in [148]. If the Additional Data was received by value, it will be sent in the EIDD by value, and if it was received by reference it will be sent in the EIDD by reference. While the Legacy PSAP Gateway does not know all of the information the primary PSAP developed in its handling of the call, it should pass what it does know to the secondary PSAP using this mechanism.

When the primary PSAP determines that it should drop off the conference and complete the transfer, it will follow the steps illustrated below.

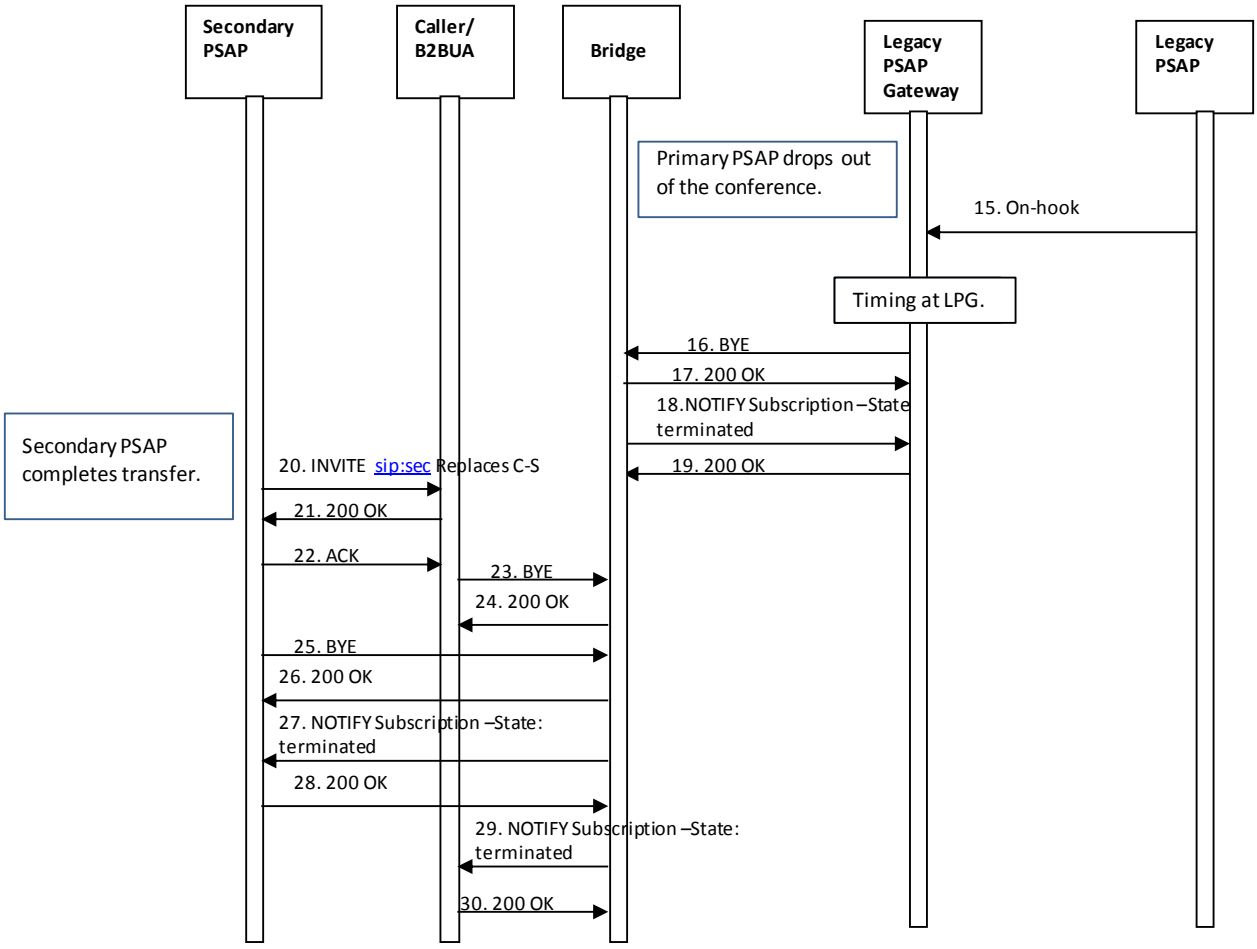



**Figure 7-5 Emergency Call Transfer Request from Legacy PSAP – Transfer Completed**

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 secondary 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 sets a timer for 1.1 seconds to distinguish a disconnect indication from a flash signal.

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. The secondary 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 secondary PSAP.
21. The caller/B2BUA responds by returning a 200 OK message.
22. The secondary 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 secondary 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 secondary PSAP.
27. The conference bridge then returns a NOTIFY message to the secondary PSAP indicating that the subscription to the conference has been terminated.
28. The secondary 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.

#### 7.2.2.5 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 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 will need to be able to replicate.

In an i3 Solution environment, a Legacy PSAP Gateway needs to 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 generates 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, where 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.

#### 7.2.2.6 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.

#### 7.2.2.7 MSRP Interworking in Support of SMS

SMS must be interworked to TTY for delivery to a legacy PSAP using its existing TTY equipment. Originated SMS messages are expected to be interworked to MSRP outside the ESInet. The NIF and/or the PIF must interwork MSRP to Baudot tones. This interwork from MSRP to TTY must be compatible with the similar function provided by the J-STD-110 Text Control Center's mapping from SMS to TTY.

Note: Further specification of interworking between MSRP and TTY will be provided in a future revision of this document.

### 7.2.3 Location Interwork Function (LIF)

As described in Section 7.2, 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 04-001 and NENA 04-005. 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 5.4.1 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 7.2.2.1) 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 will have to support the ability to query other elements (i.e., LISs, Legacy Network Gateways) using an appropriate dereferencing protocol, as specified in Section 4.2, to obtain dispatch 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 dispatch 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.

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 will need to support the HTTPS GET method described in IETF RFC 7230 [202] to obtain the Additional Data "by-value"[69]. The Legacy PSAP Gateway will 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.

[69]Legacy PSAPs do not differentiate between access networks and origination 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 origination network received via a Call-Info header field. The LPG uses the origination 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 origination networks may provide Additional Data. The LPG does not send this data to the PSAP.

### 7.2.4 Timing at the Legacy PSAP Gateway

#### 7.2.4.1 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, ANSI-0600414.1998(2007), and/or Telcordia GR-350-CORE.

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.

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).

#### 7.2.4.2 Call Disconnect Timing

Call disconnect timing depends on whether the caller[70] 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.

##### 7.2.4.2.1 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.

[70] 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.

#### 7.2.4.2.2 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 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.

### 7.2.5 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.

# 8 Data and the Emergency Incident Data Document

With the implementation of NG9-1-1 there will be many forms of additional data available to emergency responders: data associated with a call, a location, and a caller. 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. 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 Document (EIDD) and passed to other agencies that are involved with the incident.

Note: Specification for the conveyance of EIDDs between agencies, systems and applications will appear in a future revision of this document.

## 8.1 Additional Data

Any of the additional data elements in [143] or NG9-1-1 Additional Data, National Emergency Number Association, NENA 71-001 [104] or its successor document, NENA STA-012.2.201x (work

in progress) 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 usually signaled with a URI, one block per URI, although it can be passed by value in a SIP message. 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. Prior versions of this document and STA-012.2 differentiated between Additional Data about a call, caller or location. The repository for additional call data was the Call Information Database (CIDB) in version 1. In this version, there is only "Additional Data" which is provided as a series of blocks regardless of the source of the data and the Additional Data Repository holds Additional Data. Any source can provide any of the blocks defined in [143] or STA-012.2, but the following table provides examples of typical sources of blocks of Additional Data:

**Table 8-1 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 |
| CallerInfo | Caller |
| EmergencyContactInfo | Caller |
| HealthInfo | Caller |
| FloorPlanInfo | Building Owner or Tenant |

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 who 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 [143], where no originating network or service provider is in the path of the call, the calling device must provide Additional Call Data.

Every emergency call is expected to include at least one Call-Info header field with an "EmergencyCallData" prefixed purpose parameter. However, more than one Call-Info header field with an "EmergencyCallData" prefixed purpose may be received. 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.

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 will 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.

Additional Data received by reference must be passed by reference to any other entities.

### 8.2 Additional Data associated with a PSAP, the Emergency Incident Data Document

The definition of Emergency Incident Data Document (EIDD) is defined in NENA/APCO-INF-005 Emergency Incident Data Document (EIDD) Information Document [148].

When a PSAP handles a call it develops information about the call which must be passed to subsequent PSAPs dispatchers and/or responders. This structure or a reference to it will be passed with a transferred call (see section 5.8.1.3) or as part of a dispatch operation.

## 9 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.

### 9.1 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 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.

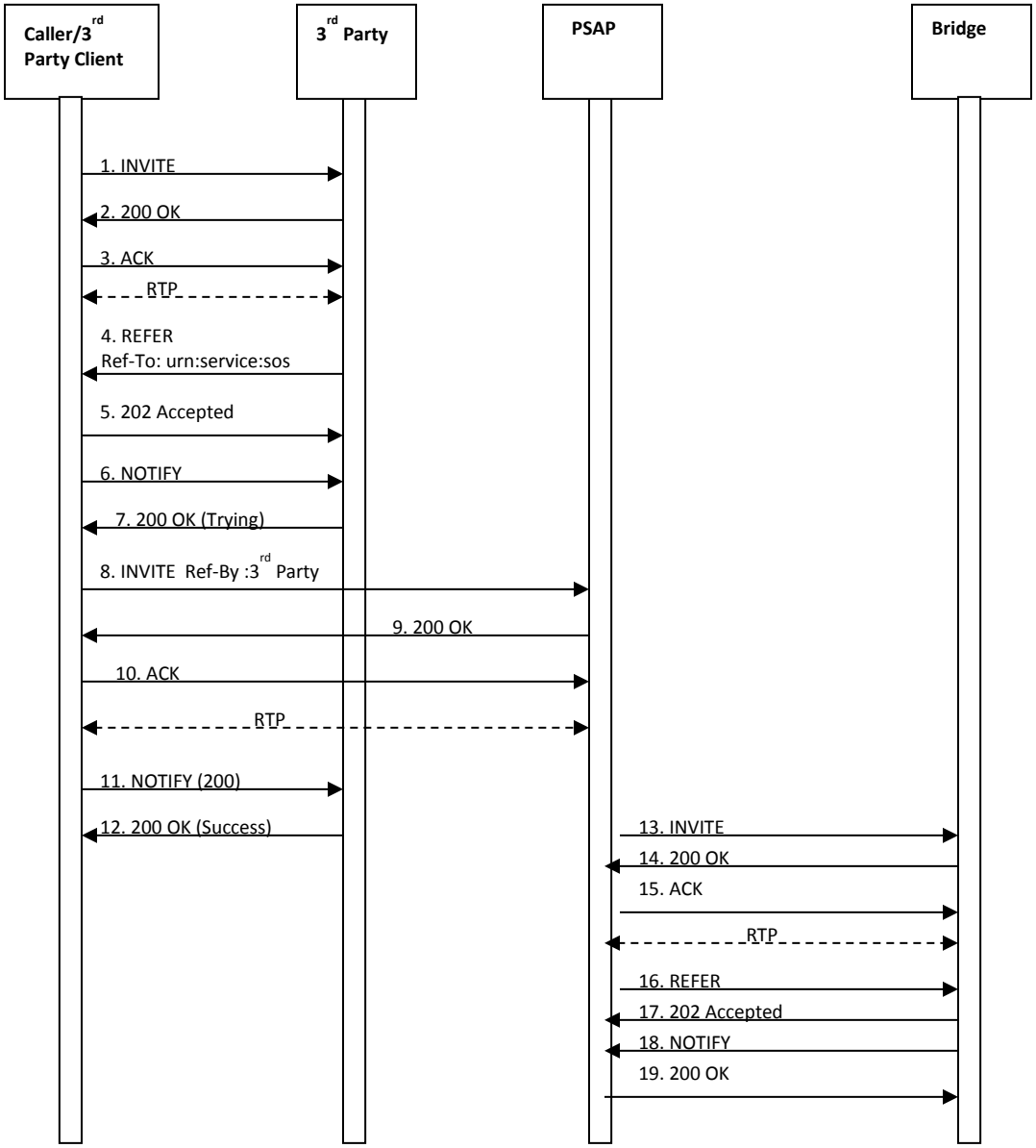



**Figure 9-1 3rd Party Origination Call Flow – PSAP Conference**

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.
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 containing the destination "urn:service:sos", that 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 202 Accepted 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 [59]. This INVITE message contains a Referred-by header 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, 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 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 202 Accepted message to the PSAP.
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.

## 9.2 3rd Party Call Agent and Caller Added to Conference

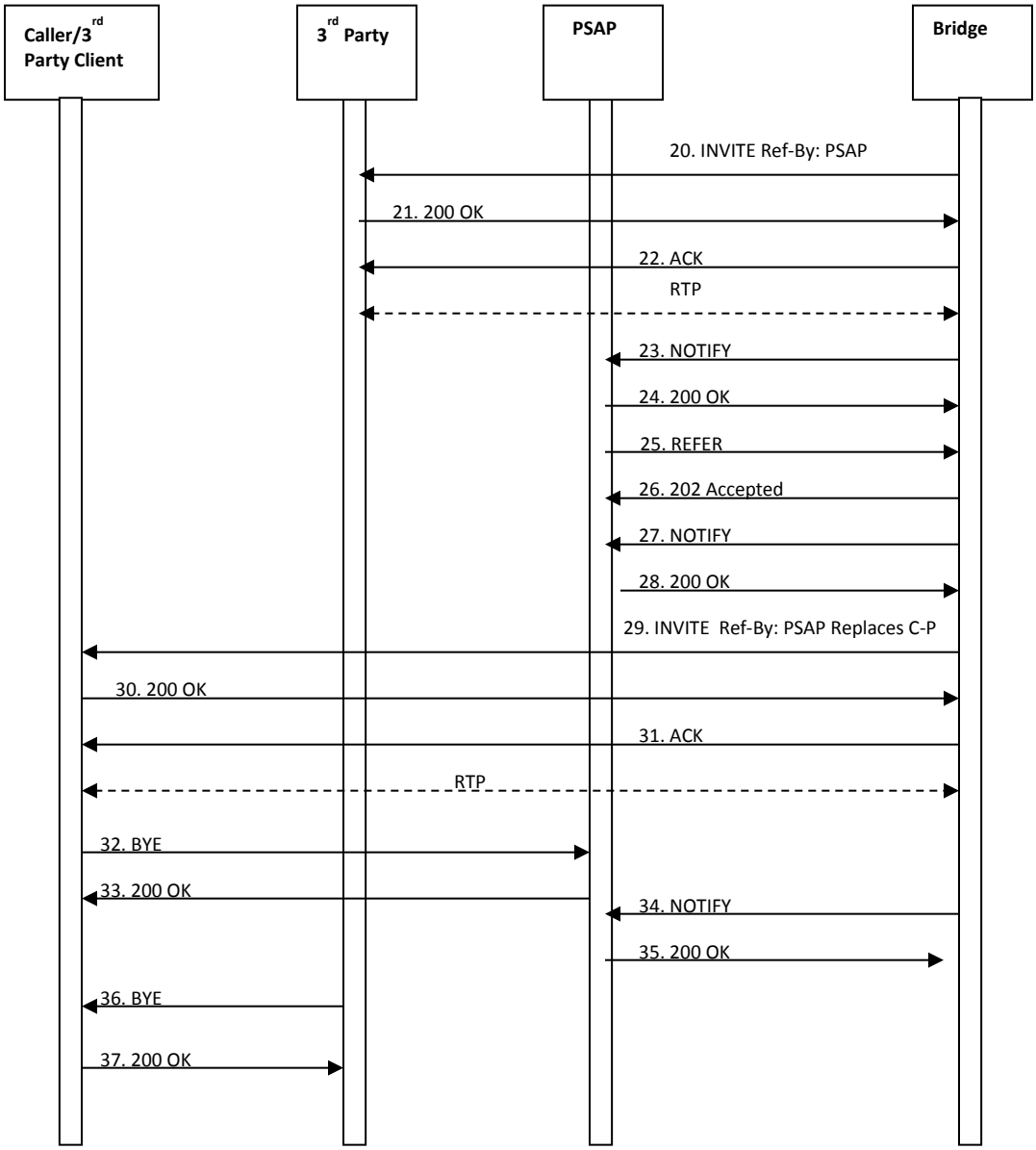



**Figure 9-2 3rd Party Call Agent - Caller Added**

20. The bridge sends an INVITE message to the 3rd party call agent. The INVITE contains an indication in a Referred-by header 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 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 202 Accepted 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 EIDD, 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.

Either the 3rd party client or the caller can initiate the disconnection of the original session between them (step 36).

# 10 Test Calls

NG9-1-1 PSAPs must implement the test function described in [59]. 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:nena: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 secondary services such as "urn:service:sos.fire.test" 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:sos.test" terminated by a CR and LF
c. The location reported with the call (in the Geolocation header). 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 domain name. 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 4474 [86]) 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 [136] 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.

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.

A PSAP Management interface will be provided in a future revision of this document.

# 11 NRS Consideration

This document requests NRS to create several registries.

## 11.1 URN Registry

The IETF has delegated to NRS the "urn:nena" namespace. NRS is requested to create a registry for "urn:nena". The "urn:nena" namespace will have a "top level" (to NRS) label, which in many cases will refer to a sub registry. For example, this document creates the "service" sub registry for "urn:nena:service". The separator between the "nena" label and the "urn" subtype ("urn:nena" registry name) is a colon ":".

In the following registries used to form URNs in the "urn:nena" namespace, occasional use of upper case letters is shown for convenience and clarity. Case is not significant when comparing "urn:nena" strings.

### 11.1.1 Name

The name of this registry is "urn:nena".

### 11.1.2 Information required to create a new value

A new entry to "urn:nena" requires an explanation of when the URN will be used, and how the new label is distinguished in its use from other URNs. It should describe who creates URNs with the label, and who uses such URNs.

### 11.1.3 Management Policy

The "NENA Standard Required" policy in NENA-STA-008.2-2014 (originally NENA 70-001) is required to add a new entry into the registry. Subregistries under "urn:nena" may not be delegated outside the control of the NRS.

### 11.1.4 Content

This registry contains:

- The UTF-8 "Name" of the "top level" label (a short string)
- The UTF-8 "Purpose" of the label (explanatory text)
- A "Subregistry" if appropriate (name of subregistry)
- A "Reference" (URI) to the NENA Standard that defines the label

### 11.1.5 Initial Values

See Section 11.2 below defining the "service" label.

This document also creates the namespace "urn:nena:xml:ns:policy:policy-v1" (see Section 4.3.2.4). The name is "policy", the "Purpose" is "route policy", there is no subregistry, and the reference is this document, "NENA-STA-010.2 (originally NENA 08-003)".

## 11.2 "service" URN Subregistry

When calls are routed within an ESInet, the routing element (PSAP or ESRP) queries the ECRF for the (nominal) route. It does so with a service URN. External routing is accomplished with "urn:service:sos", as defined by the IETF. Within the ESInet, NENA defined service URNs are used.

This document requests NRS to add a new entry to the "urn:nena" registry. The name of this entry is "service". The purpose of this entry is "Routing 9-1-1 calls within an ESInet". The "Reference" should refer to the registry created by this section, "urn:nena:service". The separator between the "service" label and the service ("urn:nena:service" registry name) is a colon ":".

Service URNs as defined here begin with "urn:nena:service". The sub-namespace defined by this registry may be further subdivided (potentially several times), by sub-registries under this sub-registry. A new entry starting with "urn:nena:service" should denote a new type of route, which must be distinguished by the PSAP or ESRP from other uses. For example, 9-1-1 calls being routed within the ESInet use "urn:nena:service:sos" (or a subspace of it). Calls routed by a PSAP to a responder use "urn:nena:service:responder" (actually, the type of responders is also included, e.g., "urn:nena:service:responder.police"). A PSAP or ESRP specifies the URN in a LoST query, the ECRF uses it to choose a (nominal) route. In this entry in the "urn:nena" registry, "service" means a path towards a service, as it does for "urn:service" as defined by the IETF.

### 11.2.1 Name

The name of this subregistry is “urn:nena:service”.

### 11.2.2 Information required to create a new value

A new entry to “urn:nena:service” requires an explanation of when the URN will be used, and how the new label is distinguished in its use from other URNs. It should describe who creates URNs with the label, and who uses such URNs.

### 11.2.3 Management Policy

The “NENA Standard Required” policy in NENA-STA-008.2-2014 (originally NENA 70-001) is required to add a new entry into the registry.

### 11.2.4 Content

This registry contains:

- The UTF-8 “Name” of the label (a short string)
- The UTF-8 “Purpose” of the label (explanatory text)
- A reference to a “Subregistry” if appropriate (name of subregistry)
- A reference (URI) to the NENA Standard that defines the label

### 11.2.5 Initial Values

This document defines the “additionalData” name, with the purpose “Return a URI to an Additional Data structure as defined in NENA 71-001” [104][71]. There is no reference. An entity such as a PSAP wishing to obtain Additional Data about a location queries the ECRF with this URN. The ECRF returns the URI to the Additional Data structure if one is available.

See section 11.3 and section 0 below for two initial additional values of this registry.

## 11.3 “urn:nena:service:sos” Registry

Routing of emergency calls within the ESInet is a primary function of this specification. When ESRPs must route calls within the ESInet, they query the ECRF for the route. Routing for emergency calls may involve multiple levels of ESRPs. Each level may need a different URN to distinguish them (it is also possible for the ECRF to distinguish by the identity of the ESRP that queries it). Routing of emergency calls, including instant messages and non-human-initiated calls, is accomplished with a URN beginning with “urn:nena:service:sos”.

NRS is requested to create an entry in the “urn:nena:service” registry with the name “sos” and with the purpose noted as “routing emergency calls within the ESInet toward a primary PSAP call taker”.

[71] A previous edition of this document defined an “AdditionalLocationData” name in this registry, which is deprecated.



One Nation 9-1-1 One Number

The reference will be to the registry created by this section, “urn:nena:service:sos”. The separator between the “sos” label and the service (“urn:nena:service:sos” registry name) is a period “.”.

The “urn:nena:service:sos” registry contains label values appropriate for the various levels of routing within the ESInet.

### 11.3.1 Name

The name of this registry is “urn:nena:service:sos”.

### 11.3.2 Information required to create a new value

A new entry to “urn:nena:service:sos” requires an explanation of when the URN will be used, and how the new label is distinguished in its use from other URNs. It should describe who creates URNs with the label, and who uses such URNs.

### 11.3.3 Management Policy

The “NENA Standard Required” policy in NENA-STA-008.2-2014 (originally NENA 70-001) is used for this registry.

### 11.3.4 Content

This registry contains:

- The UTF-8 “Name” of the label (a short string)
- The UTF-8 “Purpose” of the label (explanatory text)
- A reference (URI) to the NENA Standard that defines the label

### 11.3.5 Initial Values

| Name | Purpose | Reference |
|---|---|---|
| psap | Route calls to primary PSAP | NENA 08-003* |
| level_2_esrp | Route calls to a second level ESRP (for an example, a state ESRP routing towards a county ESRP) | NENA 08-003* |
| 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). | NENA 08-003* |
| call_taker | Route calls to a call taker within a PSAP | NENA 08-003* |

*Original document defining initial registry values; replaced by NENA-STA-010 (this document).

## 11.4 "urn:nena:service:test" Registry

Test calls are directed to "urn:service:test.sos". To route such test calls where the routing infrastructure uses multiple levels of routing, and thus uses URNs in the "urn:nena:service:sos" registry, service URNs are needed for test calls with similar levels.

NRS is requested to create an entry in the "urn:nena:service" registry with the name "test" and with the purpose noted as "routing test calls within the ESInet toward a primary PSAP". The reference will be to the registry created by this section, "urn:nena:service:test". The separator between the "test" label and the service ("urn:nena:service:test" registry name) is a period ".".

The "urn:nena:service:test" registry contains label values corresponding to the levels in the "urn:nena:service:sos" registry. These registries are normally kept in sync, an entry added to "urn:nena:service:sos" should also add a corresponding entry to urn:nena:service:test.

### 11.4.1 Name

The name of this registry is "urn:nena:service:test".

### 11.4.2 Information required to create a new value

A new entry to "urn:nena:service:test" is normally made in tandem with a new entry in the urn:nena:service:sos registry. Exceptions are allowed. The text of the standard document must clearly state how the URN will be used.

### 11.4.3 Management Policy

The "NENA Standard Required" policy in NENA-STA-008.2-2014 (originally NENA 70-001) is used for this registry.

### 11.4.4 Content

This registry contains:

- The UTF-8 "Name" of the label (a short string)
- The UTF-8 "Purpose" of the label (explanatory text)
- A reference (URI) to the NENA Standard that defines the label

### 11.4.5 Initial Values

| Name | Purpose | Reference |
|---|---|---|
| psap | Route test calls to primary PSAP | NENA-STA-010.2-2016 |
| level_2_esrp | Route test calls to a second level ESRP (for an example, a state ESRP routing towards a county ESRP) | NENA-STA-010.2-2016 |
| 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). | NENA-STA-010.2-2016 |

| Name | Purpose | Reference |
|---|---|---|
| call_taker | Normally not used, but some implementations may make use of this urn | NENA-STA-010.2-2016 |

## 11.5 "urn:nena:service:responder" Registry

Once a PSAP gets a call, they may have to transfer the call to a secondary PSAP. The secondary PSAP is chosen based on the type of responder, and the location of the caller. Routing of emergency calls from a PSAP towards a responder, including instant messages and non-human-initiated calls, is accomplished with a URN beginning with "urn:nena:service:responder".

NRS is requested to create an entry in the "urn:nena:service" registry with the name "responder" and with the purpose noted as "routing emergency calls within the ESInet towards a responder". The reference will be to the registry created by this section, "urn:nena:service:responder".

The "urn:nena:service:responder" registry contains label values appropriate for the types of responders within the ESInet. The separator between the "responder" label and the type of responder ("urn:nena:service:responder" registry name) is a period ".".

This registry is also used in other contexts where an agency type is useful. For those purposes, a 'psap' entry is provided. "urn:nena:service:agencyType.psap" must not be used to route emergency calls. It is not equivalent to, or a substitute for "urn:service:sos". Use of "urn:nena:service:agencyType.psap" is not currently defined.

### 11.5.1 Name

The name of this registry is "urn:nena:service:responder".

### 11.5.2 Information required to create a new value

A new entry to "urn:nena:service:responder" requires an explanation of the type of responder, and how it is distinguished from other responder types already in the registry.

### 11.5.3 Management Policy

The "NENA Document Required" policy in NENA-STA-008.2-2014 (originally NENA 70-001) is used for this registry.

### 11.5.4 Content

This registry contains:

- The UTF-8 "Name" of the label (a short string)
- The UTF-8 "Description" of the label (explanatory text)
- A reference (URI) to the NENA Standard that defines the label

### 11.5.5 Initial Values

| Name | Description | Reference |
|---|---|---|
| police | Police Agency | NENA 08-003* |

| Name | Description | Reference |
|---|---|---|
| fire | Fire Department | NENA 08-003* |
| ems | Emergency Medical Service | NENA 08-003* |
| poison_control | Poison Control Center | NENA 08-003* |
| mountain_rescue | Mountain Rescue Service | NENA 08-003* |
| federal_police | An appropriate federal agency (subregistry defined below) | NENA-STA-010-2016 |
| sheriff | Sheriff's office, when both a police and Sheriff dispatch may be possible | NENA 08-003* |
| stateProvincial_police | State or provincial police office | NENA 08-003* |
| coast_guard | Coast Guard station | NENA 08-003* |
| psap | other purposes beyond use for dispatch via ECRF | NENA-STA-010-2016 |

*Original document defining initial registry values; replaced by NENA-STA-010 (this document).

## 11.6 "urn:nena:service:responder.federal_police" Registry

There are several federal police agencies. This registry is a subregistry of "urn:nena:service:responder." and lists each police agency operating at the federal level.

The "urn:nena:service:responder.federal_police" registry contains label values appropriate for the types of national police responders within the ESInet. The separator between the "federal_police" label and the type of responder ("urn:nena:service:responder.federal_police" registry name) is a period ".".

### 11.6.1 Name

The name of this registry is "urn:nena:service:responder.federal_police".

### 11.6.2 Information required to create a new value

A new entry to "urn:nena:service:responder.federal_police" requires an explanation of the type of responder, and how it is distinguished from other responder types already in the registry.

### 11.6.3 Management Policy

An expert review is required to add a new entry into the registry.

### 11.6.4 Content

This registry contains:

- The UTF-8 "Name" of the label (a short string)
- The UTF-8 Full Name of the agency

### 11.6.5 Initial Values

| Name | Full Name | Reference |
|---|---|---|

| Name | Full Name | Reference |
|---|---|---|
| fbi | Federal Bureau of Investigation | NENA-STA-010.0-2016 |
| rcmp | Royal Canadian Mounted Police | NENA-STA-010.0-2016 |
| usss | U.S. Secret Service | NENA-STA-010.0-2016 |
| dea | Drug Enforcement Agency | NENA-STA-010.0-2016 |
| marshal | Marshals Service | NENA-STA-010.0-2016 |
| cbp | Customs and Border Protection | NENA-STA-010.0-2016 |
| ice | Immigration and Customs Enforcement | NENA-STA-010.0-2016 |
| atf | Bureau of Alcohol, Tobacco, Fire Arms and Explosives | NENA-STA-010.0-2016 |
| pp | U.S. Park Police | NENA-STA-010.0-2016 |
| dss | Diplomatic Security Service | NENA-STA-010.0-2016 |
| fps | Federal Protective Service | NENA-STA-010.0-2016 |

## 11.7 uid URN Subregistry

Various entities need to create globally unique identifiers. A simple way to do that is to combine a locally unique identifier and a domain name (which is globally unique). However, many entities need to create more than one type of globally unique identifier and knowing what type of identifier is helpful in diagnosing problems. For this purpose, the uid URN subregistry creates unique strings used to prepend identifiers that indicate the type of identifier it is.

### 11.7.1 Name

The name of this registry is “urn:nena:uid”.

### 11.7.2 Information required to create a new value

A new entry to “urn:nena:uid” requires an explanation of use of the identifier and the document that defines the identifier.

### 11.7.3 Management Policy

The “Document Required” policy in NENA-STA-008.2-2014 (originally NENA 70-001) is used for this registry.

### 11.7.4 Content

This registry contains:

- The UTF-8 “Name” of the identifier (a short string)
- The UTF-8 “Purpose” of the label (explanatory text)
- A reference (URI) to the document that defines the label

### 11.7.5 Initial Values

| Name | Purpose | Reference |
|---|---|---|
| callid | Call Tracking Identifier | NENA-STA-010.0-2016 |

| Name | Purpose | Reference |
|---|---|---|
| incidentid | Incident Tracking Identifier | NENA-STA-010.0-2016 |
| logid | Log Event Identifier | NENA-STA-010.0-2016 |
| lostsrc | LoST Source Identifier | NENA-STA-010.0-2016 |
| lostQuery | LoST Query Identifier | NENA-STA-010.0-2016 |

## 11.8 elementState Registry

The elementState event returns an enumerated value of the current state of an agency or element as defined in Section 3.4.2. A registry is needed to enumerate the possible values returned.

### 11.8.1 Name

The name of this registry is "elementState".

### 11.8.2 Information required to create a new value

A new entry to "elementState" requires an explanation of when value will be returned and how it is differentiated from other values in the registry.

### 11.8.3 Management Policy

The "NENA Document Required" policy in NENA NENA-STA-008.2-2014 (originally NENA 70-001) is used for this registry.

### 11.8.4 Content

This registry contains:

- The UTF-8 "Value" of the entry
- The UTF-8 "Purpose" of the entry and when it should be used
- A reference (URI) to the NENA Document that defines the label

### 11.8.5 Initial Values

The initial value and purposes of the registry are found in Section 3.4.2.

## 11.9 serviceState Registry

The "serviceState" event returns an enumerated value of the current state of a service as defined in Section 3.4.3. A registry is needed to enumerate the possible values returned.

### 11.9.1 Name

The name of this registry is "serviceState".

### 11.9.2 Information required to create a new value

A new entry to "serviceState" requires an explanation of when value will be returned and how it is differentiated from other values in the registry.

### 11.9.3 Management Policy

The "NENA Document Required" policy in NENA-STA-008.2-2014 (originally NENA 70-001) is used for this registry.

### 11.9.4 Content

This registry contains:

- The UTF-8 "Value" of the entry
- The UTF-8 "Purpose" of the entry and when it should be used
- A reference (URI) to the NENA Document that defines the label

### 11.9.5 Initial Values

The initial value and purposes of the registry are found in Section 3.4.3.

## 11.10 securityPosture Registry

The "securityPosture" event returns an enumerated value of the current security posture of an agency or element as defined in Section 3.4.1. A registry is needed to enumerate the possible values returned.

### 11.10.1 Name

The name of this registry is "securityPosture".

### 11.10.2 Information required to create a new value

A new entry to "securityPosture" requires an explanation of when value will be returned and how it is differentiated from other values in the registry.

### 11.10.3 Management Policy

The "NENA Document Required" policy in NENA-STA-008.2-2014 (originally NENA 70-001) is used for this registry.

### 11.10.4 Content

This registry contains:

- The UTF-8 "Value" of the entry
- The UTF-8 "Purpose" of the entry and when it should be used
- A reference (URI) to the NENA Document that defines the label

### 11.10.5 Initial Values

The initial value and purposes of the registry are found in Section 3.4.1. The reference is this document.

## 11.11 ExternalEventCode Registry

CAP messages are used for events sent to, and within an ESInet. CAP messages have an <event code> tag. For use within ESInets, elements sending or receiving CAP messages must have a common understanding of what kind of an event is being sent, primarily to use in routing decisions. A registry is needed for event codes defined by NENA as outlined in Section 4.1.10.

### 11.11.1 Name

The name of this registry is "ExternalEventCode".

### 11.11.2 Information required to create a new value

A new entry to "ExternalEventCode" requires an explanation of the use of the new code how it is differentiated from other values in the registry.

### 11.11.3 Management Policy

Expert Review is required to add a new entry into the registry. The Expert should consider whether the new proposed code is needed to differentiate a CAP message with that code from existing values. A proliferation of codes is not helpful because the routing mechanisms may get cumbersome. On the other hand, there are many possible sources of alerts, which may well need to be routed differentially, and thus the barrier for a new code should be modest.

### 11.11.4 Content

This registry contains:

- The UTF-8 "Value" of the entry
- The UTF-8 "Purpose" of the entry and when it should be used
- A reference to the person or document (URI) requesting the entry.

### 11.11.5 Initial Values

The registry should have the following entries:

| Value | Purpose | Reference |
|---|---|---|
| VEDS | A message from an automatic vehicle alert system containing a VEDS dataset | NENA 08-003* |
| BISACS | A message from an intelligent building or a building central alarm monitoring service containing a BISACS alert message | NENA 08-003* |

*Original document defining initial registry values; replaced by NENA-STA-010 (this document).

## 11.12 EsrpNotifyEventCode Registry

CAP messages are used for events sent to, and within an ESInet. CAP messages have an <event code> tag. For use of the "EsrpNotifyEventCode", CAP event code definitions are needed so that the

recipient of the message knows why it received the message. A registry is needed for event codes defined by NENA as outlined in Section 5.2.1.6.

### 11.12.1 Name

The name of this registry is "EsrpNotifyEventCode".

### 11.12.2 Information required to create a new value

A new entry to "EsrpNotifyEventCode" requires an explanation of the use of the new code how it is differentiated from other values in the registry.

### 11.12.3 Management Policy

Expert Review is required to add a new entry into the registry. The Expert should consider whether the new proposed code is needed to differentiate a CAP message with that code from existing values. A proliferation of codes is not helpful because interoperable implementations may get cumbersome. On the other hand, there are many possible reasons for sending these messages, which may well need to be differentiated, and thus the barrier for a new code should be modest.

### 11.12.4 Content

This registry contains:

- The UTF-8 "Value" of the entry
- The UTF-8 "Purpose" of the entry and when it should be used
- The UTF-8 "Category" that will be included in the CAP message when this event code is used
- A reference to the person or document (URI) requesting the entry.

### 11.12.5 Initial Values

The registry should have the following entries:

| Value | Purpose | Category | Reference |
|---|---|---|---|
| Normal | A normal route action was performed. This is a courtesy notification | Safety | NENA-STA-010.2-2016 |
| Default | There was insufficient location information to determine the next hop, a default was taken | Safety | NENA-STA-010.2-2016 |
| Congestion | The normal route was congested; an alternate route was taken | Safety | NENA-STA-010.2-2016 |
| Disaster | The normal destination is in disaster mode and this call was diverted | Safety | NENA-STA-010.2-2016 |
| IMR | The call met the conditions for diversion to an IMR | Safety | NENA-STA-010.2-2016 |

| Value | Purpose | Category | Reference |
|---|---|---|---|
| Busy | There were no routes available and busy was returned for this call | Safety | NENA-STA-010.2-2016 |
| Error | The ESRP encountered an error and a default route was taken | Safety | NENA-STA-010.2-2016 |
| TimeOfDay | An alternate PSAP handles calls in off hours | Safety | NENA-STA-010.2-2016 |
| GenericPolicy | Diversion occurred because of policy, not covered above | Safety | NENA-STA-010.2-2016 |
| Test | This is a test call | Safety | NENA-STA-010.2-2016 |

## 11.13 RouteCause Registry

The ESRP routes calls using its Policy Routing Function. The result of evaluating a rule set is a Route action that routes the call towards a PSAP (or responder). The Route action includes a cause value, which is placed in a Reason header associated with a History-Info header that informs the recipient why it got the call. A registry is needed for the values in the cause. The Route action cause is an enumeration, but the Reason header has a numeric cause value and a text string.

### 11.13.1 Name

The name of this registry is “RouteCause”.

### 11.13.2 Information required to create a new value

A new entry to “RouteCause” requires an explanation of the use of the new cause and how it is differentiated from other values in the registry.

### 11.13.3 Management Policy

Expert Review is required to add a new entry into the registry. There is little reason to constrain the number of entries in the Registry as long as the value definitions are distinct enough for recipients to understand why the call was received. The Expert should therefore grant new requests for values as long as the value is clearly distinct from existing values. There should not be proprietary values, i.e., values that are expressly created for a particular implementation and generally not intended to be used by other implementations. Rather the values should have wide applicability to any implementation.

### 11.13.4 Content

This registry contains:

- The UTF-8 “Value” of the entry
- The integer “Code” of the entry for the Reason header
- The UTF-8 “Text” of the entry for the Reason header
- A reference to the person or document (URI) that created the entry.

### 11.13.5 Initial Values

The registry should have the following entries:

| Value | Code | Text | Reference |
|---|---|---|---|
| Normal-NextHop | 200 | Normal Next Hop | NENA 08-003* |
| TimeOfDay | 401 | Time of Day | NENA 08-003* |
| Congestion | 402 | Congestion | NENA 08-003* |
| Disaster | 403 | Disaster | NENA 08-003* |
| IMR | 404 | Interactive Media Response | NENA 08-003* |
| GenericPolicy | 405 | Policy decision not covered above | NENA 08-003* |
| Default | 406 | Default with no/bad location | NENA 08-003* |

*Original document defining initial registry values; replaced by NENA-STA-010 (this document).

## 11.14 LogEvent Registry

Log entries have a LogEvent that specifies what kind of log record the entry contains. Log entries are defined in Section 5.13.3.2.

### 11.14.1 Name

The name of this registry is “LogEvent”.

### 11.14.2 Information required to create a new value

A new entry to “LogEvent” requires an explanation of the new value, when it would be used, and the parameters required in the log record.

### 11.14.3 Management Policy

The “NENA Document Required” policy in NENA-STA-008.2-2014 (originally NENA 70-001) is used for this registry.

### 11.14.4 Content

This registry contains:

- The UTF-8 “Value” of the entry
- The UTF-8 “Purpose” of the entry and when it should be used
- A reference (URI) to the NENA Document that defines the LogEvent

### 11.14.5 Initial Values

The initial value and purposes of the registry are found in Section 5.13.3. The reference is this document.

## 11.15 LogEvent CallSignalingMessage Protocol Registry

In the CallSignalingMessage log event, the protocol of the message must be logged. This registry provides a registry for the protocol.

### 11.15.1 Name

The name of this registry is "LogEvent CallSignalingMessage Protocol".

### 11.15.2 Information required to create a new value

A new entry to "LogEvent CallSignalingMessage Protocol" Registry requires a protocol name and a reference to a description of the protocol. The description for a proprietary protocol may be generic and not reveal proprietary information.

### 11.15.3 Management Policy

The "Expert Review" policy in NENA-STA-008.2-2014 (originally NENA 70-001) is used for this registry. The expert should ascertain that the proposed new entry is a unique protocol in the registry, is in use (or is very likely to be in use soon) for call signaling within an agency. There is no reason to constrain entries in this registry provided that new values represent distinct protocols where confusion in the logging service may occur without the new value.

### 11.15.4 Content

This registry contains:

- The UTF-8 "name" of the entry
- A reference to a document describing the protocol

### 11.15.5 Initial Values

| Name | Reference |
|---|---|
| SIP | RFC 3261 |

## 11.16 LogEvent CallTypes Registry

Call types used within the StartCall/EndCall LogEvent are listed in the "LogEvent CallTypes" Registry.

### 11.16.1 Name

The name of this registry is "LogEvent CallTypes".

### 11.16.2 Information required to create a new value

A new entry to "LogEvent CallTypes" requires a name, a definition of the call type, which must be suitably explicit to differentiate the type from existing call types, and "Primary" or "Secondary".

### 11.16.3 Management Policy

The "Expert Review" policy in NENA-STA-008.2-2014 (originally NENA 70-001) is used for this registry.

### 11.16.4 Content

This registry contains:

- The UTF-8 "name" of the entry
- A short description of the entry
- The classification ("Primary" or "Secondary")

### 11.16.5 Initial Values

| 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 |

## 11.17 LogEvent CallStates Registry

Call states used within the CallStateChange LogEvent are listed in the "LogEvent CallStates" Registry.

### 11.17.1 Name

The name of this registry is "LogEvent CallStates".

### 11.17.2 Information required to create a new value

A new entry to "LogEvent CallStates" requires a name and a definition of the call state, and must be suitably explicit to differentiate the state from existing call states. The definition must explain how <CallStateLegCallId > and <CallStateTargetID> are used with the state.

### 11.17.3 Management Policy

The "Expert Review" policy in NENA-STA-008.2-2014 (originally NENA 70-001) is used for this registry. The expert shall consider how the new state is differentiated from existing states. Too many states result in differences among implementers as to which state a call is in. Too few result in ambiguity about the actual state. The expert shall attempt to balance these forces with a bias towards simplicity.

### 11.17.4 Content

This registry contains:

- The UTF-8 "name" of the entry
- A short description of the entry

### 11.17.5 Initial Values

| Name | Description |
|---|---|
| beginCall | Indicates the start of a new call. If the call is also a SIP call, the StartCall 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. |
| endCall | Indicates the end of a call. If the call is also a SIP call, the EndCall LogEvent must be logged. < CallStateLegCallId > and <CallStateTargetID> must not be supplied. |
| callCancel | A cancel request has been received for the call. < CallStateLegCallId > and <CallStateTargetID> must not be supplied. |
| holdCall | 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. |
| parkCall | 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. |
| retrieveCall | Indicates that a held or parked call has been re-activated. < CallStateLegCallId > and <CallStateTargetID> must not be supplied. |
| addParty | 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 >. |
| removeParty | 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. |
| bargeInCall | 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. |

## 11.18 AgencyRoles Registry

Agencies are classified by a role in the ESInet.

### 11.18.1 Name

The name of this registry is "AgencyRoles".

### 11.18.2 Information required to create a new value

A new entry to "AgencyRoles" requires a definition of the role, and must be suitably explicit to differentiate the role from existing roles.

### 11.18.3 Management Policy

The "NENA Document Required" policy in NENA-STA-008.2-2014 (originally NENA 70-001) is used for this registry.

### 11.18.4 Content

This registry contains:

- The UTF-8 "role" of the entry
- A reference (URI) to the NENA Document that defines the role

### 11.18.5 Initial Values

The initial roles are found in Section 6.3. The role entry in the registry should be in "camelCase", thus "ESInet Operator" as listed in Section 6.3 should be "ESInetOperator" in the registry. The reference is this document.

## 11.19 AgentRoles Registry

Agents authenticate to the ESInet in one or more roles. The roles are defined in a NENA Information Document to be referenced in a future revision of this document.

### 11.19.1 Name

The name of this registry is "AgentRoles".

### 11.19.2 Information required to create a new value

A new entry to "AgentRoles" requires a definition of the role, and must be suitably explicit to differentiate the role from existing roles.

### 11.19.3 Management Policy

The "NENA Document Required" policy in NENA-STA-008.2-2014 (originally NENA 70-001) is used for this registry. Normally, this will be a revision to a specific NENA Information Document (to be created) that defines all NG9-1-1 agent roles.

### 11.19.4 Content

This registry contains:

- The UTF-8 "role" of the entry
- A reference (URI) to the NENA Document that defines the role

### 11.19.5 Initial Values

The initial roles are found in Section 6.3. The role entry in the registry should be in "camelCase", thus "Shift Supervisor" as listed in Section 6.3 should be "shiftSupervisor" in the registry. The reference is this document.

## 11.20 e Agent States

An agent may be in one of several states. The Agent State registry enumerates the states an agent can be in. These values are used, among other places in the AgentStateChange log event.

### 11.20.1 Name

The name of this registry is "AgentStates".

### 11.20.2 Information required to create a new value

A new entry to "AgentStates" requires a definition of the state, and must be suitably explicit to differentiate the state from existing states.

### 11.20.3 Management Policy

The "Expert Review" policy in NENA-STA-008.2-2014 (originally NENA 70-001) is used for this registry. The Expert shall balance the need to differentiate agents between roles with the inability of implementations and agencies to decide which state and agent is in. The expert should bias towards simplicity, but not at the expense of clarity.

### 11.20.4 Content

This registry contains:

- The UTF-8 "state" of the agent
- A description that defines the state

### 11.20.5 Initial Values

| Name | Description |
|---|---|
| LoggedOut | Not currently logged in to the queue |
| Break | Not at the console and unavailable to take a call |
| Waiting | Not engaged |
| Active | On a call |
| Hold | On a call, have the call on hold |
| Reserved | Temporarily being alerted to receive a specific call, not ready to take another. Will transition to Active when call is answered. |

## 11.21 "urn:nena:service:agencyLocator" Registry

To find information about an agency in the ESInet, an Agency Locator function is described in Section 5.16. A search function for the Agency Locator is described in Section 5.16.2, which uses a service URN in the ECRF. A search for an agency locator record URI is accomplished with a URN beginning with "urn:nena:service:agencyLocator".

NRS is requested to create an entry in the "urn:nena:service" registry with the name "agencyLocator" and with the purpose noted as "finding an agency locator record". The reference will be to the registry created by this section, "urn:nena:service:agencyLocator".

The "urn:nena:service:agencyLocator" registry contains label values appropriate for the types of agencies within the ESInet. The separator between the "agencyLocator" label and the type of agency (urn:nena:service:agencyLocator registry name) is a period ".".

### 11.21.1 Name

The name of this registry is "urn:nena:service:agencyLocator".

### 11.21.2 Information required to create a new value

A new entry to "urn:nena:service:agencyLocator" requires an explanation of the type of agency, and how it is distinguished from other agency types already in the registry.

### 11.21.3 Management Policy

The "NENA Document Required" policy in NENA-STA-008.2-2014 (originally NENA 70-001) is used for this registry. In addition, when an entry is made in the "urn:nena:service:responder" registry, a corresponding entry will be made in this registry.

### 11.21.4 Content

This registry contains:

- The UTF-8 "Name" of the label (a short string)

- The UTF-8 "Purpose" of the label (explanatory text)
- A reference (URI) to the NENA Standard that defines the label

### 11.21.5 Initial Values

| Name | Purpose | Reference |
|---|---|---|
| psap | Primary Answering point for 911 calls | NENA-STA-010.2-2016 |
| eoc | Emergency Operations Center | NENA-STA-010.2-2016 |

In addition, all current values of the "urn:nena:service:responder" registry will be included in this registry, with the same Purpose and reference values.

## 11.22 Identity Searchable Additional Data Repository Registry

IS-ADRs are queried by ESRPs, PSAPs and other agencies and elements when Additional Data is supplied by an entity not in the call path or access network. There may be more than one IS-ADR. A potential caller selects the IS-ADR to hold their information. Agencies and elements needing Additional Data supplied by entities not in the call path or access network must query all IS-ADRs to find the data. This registry contains URIs for all IS-ADRs. See Section 5.11.1.

### 11.22.1 Name

The name of this registry is "IS-ADR".

### 11.22.2 Information required to create a new value

The URI to which queries to the IS-ADR are directed.

### 11.22.3 Management Policy

First Come First Served.

Note: If the number of IS-ADRs becomes large, NENA will modify the management policy to restrict the number of IS-ADRs, and references from unrecognized (not in the registry) IS-ADRs to an IS-ADR in the registry may be required in order to balance choice of the potential caller and the complexity of how many queries are needed to resolve the IS-ADR that holds the data from the information in the call. An unrecognized IS-ADR would have to enter into a relationship with a registered IS-ADR to allow the reference to occur.

### 11.22.4 Content

This registry contains:

- URI to the IS-ADR
- Contact vCard for the IS-ADR operator

### 11.22.5 Initial Values

There are no initial values.

## 11.23 SIPheader 'Is' Operator conditions

In a route policy SIPheader condition, the "Is" operator can test a header value for certain conditions. This registry defines the possible conditions for "Is". See Section 4.3.2.1.2.

### 11.23.1 Name

The name of this registry is "SIPheaderIsOperatorConditions".

### 11.23.2 Information required to create a new value

The new name and description of the condition that is to be tested. New values must have clear differentiation from current values.

### 11.23.3 Management Policy

The "NENA Standard Required" policy in NENA-STA-008.2-2014 (originally NENA 70-001) is used for this registry.

### 11.23.4 Content

This registry contains:

- The name of the condition to be tested, which would appear in the policy
- A short description of what would be tested
- A reference to the document that describes the condition

### 11.23.5 Initial Values

| Name | Description | Reference |
|---|---|---|
| missing | The header is not present | NENA-STA-010.2-2016 |
| erroneous | The header syntactically incorrect, or there is another error detected in it | NENA-STA-010.2-2016 |

## 11.24 Logging Service Media Error Reason Codes Registry

If an error is encountered in logging media, a log event with an error code is logged. The error codes are defined in this registry.

### 11.24.1 Name

The name of this registry is "LoggingServiceMediaErrorReasonCodes".

### 11.24.2 Information required to create a new value

The new name and description of the condition that is to be defined. New values must have clear differentiation from current values.

### 11.24.3 Management Policy

The "Expert Review" policy in NENA-STA-008.2-2014 (originally NENA 70-001) is used for this registry.

### 11.24.4 Content

This registry contains:

- The name of the code
- A short description of the code
- A reference to the document that describes the condition

### 11.24.5 Initial Values

| Name | Description | Reference |
|---|---|---|
| lostConnection | The connection to the SRS was lost and could not be re-established | NENA-STA-010.2-2016 |
| dropOuts | There were significant number of missing media packets | NENA-STA-010.2-2016 |

## 11.25 "urn:nena:xml" Registry

When NENA documents create XML objects, namespaces and schemas for those objects need to be unique and defined by a URI. This registry contains the top-level names for the two subregistries (namespace and schema) and the procedures for creating new namespaces.

This registry defines a two level naming convention. Each registration is within a category, and the namespace is defined within one such category.

### 11.25.1 Name

The name of this registry is "urn:nena:xml".

### 11.25.2 Information required to create a new value

The name and description of the new category of XML information that is to be defined. New values must have clear differentiation from current values.

### 11.25.3 Management Policy

The "NENA Standard Required" policy in NENA-STA-008.2-2014 (originally NENA 70-001) is used for this registry.

### 11.25.4 Content

This registry contains:

- The name of the subregistry
- A short description of the subregistry

- A reference to the document that describes the subregistry

### 11.25.5 Initial Values

| Name | Description | Reference |
|---|---|---|
| ns | Namespace | NENA-STA-010.2-2016 |
| schema | XML Schema | NENA-STA-010.2-2016 |

## 11.26 urn:nena:xml:ns Registry

Defines a stable reference URI for an XML object. This registry defines a two-level naming convention. Each registration is within a category, and the namespace is defined within one such category. The separator between the category and the name is a period.

### 11.26.1 Name

The name of this registry is "urn:nena:xml:ns".

### 11.26.2 Information required to create a new value

Category and specific name for the namespace. When a new category is to be created, the reasons why a new one is appropriate should be supplied to the expert reviewer.

### 11.26.3 Management Policy

The "Expert Review" policy in NENA-STA-008.2-2014 (originally NENA 70-001) is used for this registry. The expert should consider only the category. A new category should be created only when existing categories are not appropriate. The Expert should encourage objects that are related to have the same category, but, as categories are not expensive, new ones should be created when there is sufficient justification to do so.

### 11.26.4 Content

This registry contains:

- The category
- The object name
- A reference to the document that describes the subregistry

### 11.26.5 Initial Values

| Category | Name | Reference |
|---|---|---|
| securityPosture | subscribe | NENA-STA-010.2-2016 |
| securityPosture | notify | NENA-STA-010.2-2016 |
| elementState | subscribe | NENA-STA-010.2-2016 |
| elementState | notify | NENA-STA-010.2-2016 |
| serviceState | subscribe | NENA-STA-010.2-2016 |
| serviceState | notify | NENA-STA-010.2-2016 |

| Category | Name | Reference |
|---|---|---|
| policy | retrievePolicyRequest | NENA-STA-010.2-2016 |
| policy | retrievePolicyResponse | NENA-STA-010.2-2016 |
| policy | moreRetrievePolicyRequest | NENA-STA-010.2-2016 |
| policy | moreRetrievePolicyResponse | NENA-STA-010.2-2016 |
| policy | storePolicyRequest | NENA-STA-010.2-2016 |
| policy | storePolicyResponse | NENA-STA-010.2-2016 |
| policy | moreStorePolicyRequest | NENA-STA-010.2-2016 |
| policy | moreStorePolicyResponse | NENA-STA-010.2-2016 |
| policy | enumeratePoliciesRequest | NENA-STA-010.2-2016 |
| policy | enumeratePoliciesResponse | NENA-STA-010.2-2016 |
| policy | updatedPolicyRequest | NENA-STA-010.2-2016 |
| policy | updatedPolicyResponse | NENA-STA-010.2-2016 |
| policy | policy-v1 | NENA-STA-010.2-2016 |
| dr | discrepancyReportRequest | NENA-STA-010.2-2016 |
| dr | discrepancyReportResponse | NENA-STA-010.2-2016 |
| lostExt | callIncidentIds | NENA-STA-010.2-2016 |

## 11.27 urn:nena:xml:schema Registry

Defines a stable reference location for schemas. This registry uses the same two-level naming scheme of “urn:nena:xml:ns”. The separator between the category and the name is a period.

### 11.27.1 Name

The name of this registry is “urn:nena:xml:schema”.

### 11.27.2 Information required to create a new value

Category and specific name for an existing or new namespace. The category and name must be created in “urn:nena:xml:ns” before, or simultaneously with the creation of the “urn:nena:xml:schema” entry.

### 11.27.3 Management Policy

The “Expert Review” policy in NENA-STA-008.2-2014 (originally NENA 70-001) is used for this registry. The expert shall assure that the namespace exists, or is being created simultaneously and that the schema can be validated.

### 11.27.4 Content

This registry contains:

- The category
- The object name
- A reference to the document that describes the subregistry
- A stable URI that points to the schema, within the NRS.

### 11.27.5 Initial Values

None.

## 11.28 Status Codes Registry

When web services return status codes, the code must be listed in the Status Codes registry.

### 11.28.1 Name

The name of this registry is "StatusCodes".

### 11.28.2 Information required to create a new value

The code, which must be numeric and unique in the registry, a short description and the document that defined the status code are required.

### 11.28.3 Management Policy

The "NENA Document Required" policy in NENA-STA-008.2-2014 (originally NENA 70-001) is used for this registry.

### 11.28.4 Content

This registry contains:

- The status code
- A short description if not obvious from the name
- A reference (URI) to the document that describes the code

### 11.28.5 Initial Values

| Status Code | Description | Reference |
|---|---|---|
| 200 | Okay | NENA-STA-010.2-2016 |
| 303 | Iterative Refer | NENA-STA-010.2-2016 |
| 501 | Unknown or bad Policy Name | NENA-STA-010.2-2016 |
| 502 | Unknown or bad Agency Name | NENA-STA-010.2-2016 |
| 503 | Not available here, no referral available | NENA-STA-010.2-2016 |
| 504 | Unspecified Error | NENA-STA-010.2-2016 |
| 505 | Bad chunkId | NENA-STA-010.2-2016 |
| 506 | Bad queue | NENA-STA-010.2-2016 |
| 507 | Bad dequeuePreference | NENA-STA-010.2-2016 |
| 508 | Policy Violation | NENA-STA-010.2-2016 |
| 509 | Policy Too Large | NENA-STA-010.2-2016 |
| 510 | Bad TTL | NENA-STA-010.2-2016 |
| 511 | Chunk Too Big | NENA-STA-010.2-2016 |
| 512 | No Address Found | NENA-STA-010.2-2016 |

| | | |
|---|---|---|
| 513 | No such sourceId | NENA-STA-010.2-2016 |
| 514 | Unauthorized | NENA-STA-010.2-2016 |
| 515 | Unknown MCS/GCS | NENA-STA-010.2-2016 |
| 516 | No such callIdentifier | NENA-STA-010.2-2016 |
| 517 | No such incidentIdentifier | NENA-STA-010.2-2016 |
| 518 | Bad Timestamp | NENA-STA-010.2-2016 |
| 519 | No such logtIdentifier | NENA-STA-010.2-2016 |
| 520 | EndTime occurs before StartTime | NENA-STA-010.2-2016 |
| 521 | Bad or missing Geoshape | NENA-STA-010.2-2016 |
| 522 | Unknown Service/Database (“not ours”) | NENA-STA-010.2-2016 |
| 523 | Unauthorized Reporter | NENA-STA-010.2-2016 |
| 524 | Unknown ReportId | NENA-STA-010.2-2016 |
| 525 | Bad Query Key | NENA-STA-010.2-2016 |
| 526 | No Data Found | NENA-STA-010.2-2016 |
| 527 | Bad Log Event | NENA-STA-010.2-2016 |
| 528 | Event too big | NENA-STA-010.2-2016 |
| 529 | Event not on whitelist | NENA-STA-010.2-2016 |
| 530 | Event on blacklist | NENA-STA-010.2-2016 |
| 531 | Timeout | NENA-STA-010.2-2016 |
| 532 | Malformed or Invalid Data | NENA-STA-010.2-2016 |
| 533 | Lost Connection | NENA-STA-010.2-2016 |

## 11.29 Interface Names Registry

Interface names for use with data rights management policies, as described in Section 6.5 are contained in the “InterfaceNames” Registry.

### 11.29.1 Name

The name of this registry is “InterfaceNames”.

### 11.29.2 Information required to create a new value

The name of the interface and the document that describes it.

### 11.29.3 Management Policy

The “Document Required” and “Expert Review” policies in NENA-STA-008.2-2014 (originally NENA 70-001) are used for this registry. The Expert should determine that the interface is suitably documented and named and is appropriate to have data rights management policy applied.

### 11.29.4 Content

This registry contains:

- The interface name

- A reference to the document that describes the subregistry

### 11.29.5 Initial Values

| Name | Reference |
|---|---|
| SIPcall | NENA-STA-010.2-2016 |
| LoST | NENA-STA-010.2-2016 |
| ElementState | NENA-STA-010.2-2016 |
| ServiceState | NENA-STA-010.2-2016 |
| SecurityPosture | NENA-STA-010.2-2016 |
| HELDdereference | NENA-STA-010.2-2016 |
| SIMPLEpresence | NENA-STA-010.2-2016 |
| PolicyStore | NENA-STA-010.2-2016 |
| DiscrepancyReport | NENA-STA-010.2-2016 |
| QueueState | NENA-STA-010.2-2016 |
| DequeueRegistration | NENA-STA-010.2-2016 |
| ESRPNotify | NENA-STA-010.2-2016 |
| AbandonedCall | NENA-STA-010.2-2016 |
| SI | NENA-STA-010.2-2016 |
| GapOverlap | NENA-STA-010.2-2016 |
| PIDFLOtoMSAG | NENA-STA-010.2-2016 |
| MSAGtoPIDFLO | NENA-STA-010.2-2016 |
| Geocode | NENA-STA-010.2-2016 |
| ReverseGeocode | NENA-STA-010.2-2016 |
| ConferenceEvent | NENA-STA-010.2-2016 |
| Logging | NENA-STA-010.2-2016 |
| SIPREC | NENA-STA-010.2-2016 |
| LoggingRetrieval | NENA-STA-010.2-2016 |
| AgencyLocatorDereference | NENA-STA-010.2-2016 |
| AgencyLocatorNameSearch | NENA-STA-010.2-2016 |
| MapDatabase | NENA-STA-010.2-2016 |
| LNGadr | NENA-STA-010.2-2016 |

## 11.30 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.

### 11.30.1 RelaxNG Schema

namespace a = "http://relaxng.org/ns/compatibility/annotations/1.0"

default namespace ns1 = "urn:nena:xml:ns:lostExt:Ids"

## Location-to-Service Translation (LoST) Protocol Extension

## Add CallId and IncidentTrackingId to LoST requests

```
##      This object goes in the extensionPoint in the commonRequestPattern
start =   nenaCallIncidentId
div {
nenaCallIncidentId =     element nenaCallIncidentId {
      attribute callId { xsd:token },  attribute incidentTrackingId  { xsd:token } }
}
```

### 11.31 Too Many Mappings Warning Extension to LoST

This document defines an extension to LoST, which adds a Too Many Mappings warning to a <findServiceResponse>.

#### 11.31.1 RelaxNG Schema

```
namespace a = "http://relaxng.org/ns/compatibility/annotations/1.0"
namespace b =  "urn:ietf:params:xml:ns:lost1"
default namespace ns1 = "urn:nena:xml:ns:lostExt"
## Location-to-Service Translation (LoST) Protocol Extension
##       TooManyMappings as a warning
##      This object goes in the extensionPoint in the exceptionContainer of
##       findservice
start =  tooManyMappings
div {
tooManyMappings = element tooManyMappings { b:basicException }
}
```

## 12 IANA Actions

### 12.1 SDP parameter “suspended”.

Per Appendix C, IANA is requested to add “suspended” to the subregistry “att-field” in the “Session Description Protocol (SDP) Parameters” registry. The Type is “att-field (both session and media level)”, the SDP Name is “suspended”, and the Reference is this document.

## 13 Documentation Required for the Development of a NENA XML Schema

Schemas were already completed before new template developed.  This section will be updated to include all schemas with the next version of this document.

# 14 Recommended Reading and 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. i3 Technical Requirements Document, National Emergency Number Association, NENA 08-751
2. NENA Master Glossary of 9-1-1 Terminology, National Emergency Number Association, NENA 00-001
3. Interim VoIP Architecture for Enhanced 9-1-1 Services (i2), National Emergency Number Association, NENA 08-001
4. Framework for Emergency Calling in Internet Multimedia, B. Rosen, J. Polk, H. Schulzrinne, A. Newton, Internet Engineering Task Force, RFC 6443
5. Geopriv Requirements, J. Cueller et al., Internet Engineering Task Force, RFC 3693
6. A Presence-based GEOPRIV Location Object Format, J. Peterson, Internet Engineering Task Force, RFC 4119
7. Dynamic Host Configuration Protocol Option for Coordinate-based Location Configuration Information, J. Polk, J. Schnizlein, M. Linsner, Internet Engineering Task Force, RFC 3825
8. Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) Option for Civic Addresses Configuration Information, H. Schulzrinne, Internet Engineering Task Force, RFC 4776
9. HTTP Enabled Location Delivery (HELD) M. Barnes, ed., Internet Engineering Task Force, RFC 5985
10. Session Initiation Protocol Location Conveyance, J. Polk, B. Rosen, Internet Engineering Task Force, RFC 6442
11. A Hitchhikers Guide to the Session Initiation Protocol (SIP), J. Rosenberg, Internet Engineering Task Force, RFC 5411
12. Session Initiation Protocol, J, Rosenberg et al., Internet Engineering Task Force, RFC 3261
13. RTP: A Transport Protocol for Real-Time Applications, H. Schulzrinne et al., Internet Engineering Task Force, RFC 3550
14. SDP: Session Description Protocol, J. Handley, V. Jacobson, Internet Engineering Task Force, RFC 4566
15. Session Initiation Protocol (SIP): Locating SIP Servers, J. Rosenberg, H. Schulzrinne, Internet Engineering Task Force, RFC 3263
16. An Offer/Answer Model with the Session Description Protocol (SDP), J. Rosenberg, H. Schulzrinne, Internet Engineering Task Force, RFC 3264
17. Session Initiation Protocol (SIP)-Specific Event Notification, A. Roach, Internet Engineering Task Force, RFC 3265

18. The Session Initiation Protocol UPDATE Method, J. Rosenberg, Internet Engineering Task Force, RFC 3311
19. A Privacy Mechanism for the Session Initiation Protocol (SIP), J. Peterson, RFC 3323
20. Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks, C. Jennings, J. Peterson, M. Watson, Internet Engineering Task Force, RFC 3325
21. Session Initiation Protocol (SIP) Extension for Instant Messaging, B. Campbell et al., Internet Engineering Task Force, RFC 3428
22. The Reason Header Field for the Session Initiation Protocol (SIP), H. Schulzrinne, D. Oran, G. Camarillo, Internet Engineering Task Force, RFC 3326
23. The Session Initiation Protocol (SIP) Refer Method, R. Sparks, Internet Engineering Task Force, RFC 3515
24. Grouping of Media Lines in the Session Description Protocol (SDP), G. Camarillo et al., Internet Engineering Task Force, RFC 3388
25. An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing, J. Rosenberg, H. Schulzrinne, Internet Engineering Task Force, RFC 3581
26. Real Time Control Protocol (RTCP) attribute in Session Description Protocol (SDP), C. Huitema, Internet Engineering Task Force, RFC 3605
27. Control of Service Context using SIP Request-URI, B. Campbell, R. Sparks, Internet Engineering Task Force, RFC 3087
28. Connected Identity in the Session Initiation Protocol (SIP), J. Elwell, Internet Engineering Task Force, RFC 4916
29. Indicating User Agent Capabilities in the Session Initiation Protocol (SIP), J. Rosenberg, H. Schulzrinne, P. Kyzivat, Internet Engineering Task Force, RFC 3840
30. Caller Preferences for the Session Initiation Protocol (SIP), J. Rosenberg, H. Schulzrinne, P. Kyzivat, Internet Engineering Task Force, RFC 3841
31. A Presence Event Package for the Session Initiation Protocol (SIP), J. Rosenberg, Internet Engineering Task Force, RFC 3856
32. A Watcher Information Event Template-Package for the Session Initiation Protocol (SIP), J. Rosenberg, Internet Engineering Task Force, RFC 3857
33. The Session Initiation Protocol (SIP) "Replaces" Header, R. Mahy, B. Biggs, R. Dean, Internet Engineering Task Force, RFC 3891
34. The Session Initiation Protocol (SIP) Referred-By Mechanism, R. Sparks, Internet Engineering Task Force, RFC 3892
35. Best Current Practices for Third Party Call Control (3pcc) in the Session Initiation Protocol (SIP), J. Rosenberg et al., Internet Engineering Task Force, RFC 3725

36. Using E.164 numbers with the Session Initiation Protocol (SIP), J. Peterson et al., Internet Engineering Task Force, RFC 3824
37. Early Media and Ringing Tone Generation in the Session Initiation Protocol (SIP), G. Camarillo, H. Schulzrinne, Internet Engineering Task Force, RFC 3960
38. Presence Information Data Format (PIDF), H. Sugano, Internet Engineering Task Force, RFC 3863
39. Session Timers in the Session Initiation Protocol (SIP), S. Donovan, J. Rosenberg, Internet Engineering Task Force, RFC 4028
40. Internet Media Type message/sipfrag, R. Sparks, Internet Engineering Task Force, RFC 3420
41. The Session Initiation Protocol (SIP) "Join" Header, R. Mahy, D. Petrie, Internet Engineering Task Force, RFC 3911
42. Transcoding Services Invocation in the Session Initiation Protocol (SIP) Using Third Party Call Control (3pcc), G. Camarillo et al., Internet Engineering Task Force, RFC 4117
43. Basic Network Media Services with SIP, J. Berger et al., Internet Engineering Task Force, RFC 4240
44. An Extension to the Session Initiation Protocol (SIP) for Request History Information, M. Barnes et al., Internet Engineering Task Force, RFC 4244
45. Actions Addressing Identified Issues with the Session Initiation Protocol's (SIP) Non-INVITE Transaction, R. Sparks, Internet Engineering Task Force, RFC 4320
46. Extending the Session Initiation Protocol (SIP) Reason Header for Preemption Events, J. Polk, Internet Engineering Task Force, RFC 4411
47. Communications Resource Priority for the Session Initiation Protocol (SIP), H. Schulzrinne, J. Polk, Internet Engineering Task Force, RFC 4412
48. Suppression of Session Initiation Protocol (SIP) REFER Method Implicit Subscription, O. Levin, Internet Engineering Task Force, RFC 4488
49. Conveying Feature Tags with the Session Initiation Protocol (SIP) REFER Method, O. Levin, A. Johnston, Internet Engineering Task Force, RFC 4508
50. Addressing an Amplification Vulnerability in Session Initiation Protocol (SIP) Forking Proxies, R. Sparks et al., RFC 5393
51. Session Initiation Protocol Call Control - Conferencing for User Agents, A. Johnston, O. Levin, Internet Engineering Task Force, RFC 4579
52. A Session Initiation Protocol (SIP) Event Package for Conference State, R. Rosenberg, H. Schulzrinne, O. Levin, Internet Engineering Task Force, RFC 4575
53. Obtaining and Using Globally Routable User Agent (UA) URIs (GRUU) in the Session Initiation Protocol (SIP), J. Rosenberg, Internet Engineering Task Force, RFC 5627

54. Managing Client Initiated Connections in the Session Initiation Protocol (SIP), C. Jennings et al., Internet Engineering Task Force, RFC 5626

55. SDP: Session Description Protocol, M. Handley et. al, Internet Engineering Task Force, RFC 4566

56. Session Initiation Protocol Package for Voice Quality Reporting, A. Pendleton et al., Internet Engineering Task Force, RFC 6035

57. Interactive Connectivity Establishment (ICE): A Methodology for Network Address Translator (NAT) Traversal for Offer/Answer Protocols, J. Rosenberg, Internet Engineering Task Force, RFC 5245

58. A Uniform Resource Name (URN) for Emergency and Other Well-Known Services, H. Schulzrinne, Internet Engineering Task Force, RFC 5031

59. Best Current Practice for Communications Services in support of Emergency Calling, B. Rosen, J. Polk, Internet Engineering Task Force, RFC 6881

60. Location-to-URL Mapping Architecture and Framework, H. Schulzrinne, Internet Engineering Task Force, RFC 5582

61. LoST: A Location-to-Service Translation Protocol, T. Hardie et al., Internet Engineering Task Force, RFC 5222

62. A Framework for Centralized Conferencing, M. Barnes, C. Boulton, O. Levin, Internet Engineering Task Force, RFC 5239

63. Conference Information Data Model for Centralized Conferencing (XCON), O. Novo, G. Camarillo, D. Morgan, E. Even, Internet Engineering Task Force, RFC 6501

64. IP Multimedia Subsystem (IMS) emergency sessions, 3rd Generation Partnership Project, 3GPP TS 23.167

65. General Packet Radio Service (GPRS); Service description; Stage 2, 3rd Generation Partnership Project, 3GPP TS 23.060

66. IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3, 3rd Generation Partnership Project, 3GPP TS 23.229

67. ATIS Next Generation Network (NGN) Framework, Part III: Standards Gap Analysis, Alliance for Telecommunications Industry Solutions, May 2006

68. IP Network-to-Network Interface (NNI) Standard for VoIP, Alliance for Telecommunications Industry Solutions, ATIS-PP-1000009.2006

69. Enhanced Wireless 9-1-1 Phase 2, Telecommunications Industry Association and Alliance for Telecommunications Industry Solutions, J-STD-036-B

70. Universal Description, Discovery and Integration (UDDI) Version 3.0, Organization for the Advancement of Structured Information Standards (OASIS), UDDI V3.0

71. OASIS UDDI Specifications TC - Committee Best Practices, Organization for the Advancement of Structured Information Standards (OASIS), UDDI Best Practices

72. OASIS UDDI Specifications TC - Committee Technical Notes, Organization for the Advancement of Structured Information Standards (OASIS), UDDI Technical Notes

73. NENA Technical Requirements Document for Location Information to Support IP-Based Emergency Services, NENA 08-752, Issue 1

74. NENA Recommended Method(s) for Location Determination to Support IP-Based Emergency Services - Technical Information Document, NENA 08-505, Issue 1

75. GEOPRIV Presence Information Data Format Location Object (PIDF-LO) Usage Clarification, Considerations, and Recommendations, J. Winterbottom, M. Thomson, H. Tschofenig, Internet Engineering Task Force, RFC 5491

76. Revised Civic Location Format for Presence Information Data Format Location Object (PIDF-LO), M. Thomson, J. Winterbottom, Internet Engineering Task Force, RFC 5139

77. Requirements for a Location-by-Reference Mechanism used in Location Configuration and Conveyance, R. Marshall, Internet Engineering Task Force, RFC 5808

78. A Location Dereferencing Protocol Using HTTP-Enabled Location Delivery (HELD), J. Winterbottom et al., Internet Engineering Task Force, RFC 6753

79. Session Initiation Protocol (SIP) Overload Control, V. Gurbani, V. Hilt, H. Schulzrinne, Internet Engineering Task Force, RFC 7339

80. Lightweight Directory Access Protocol (v3), M. Wahl, T. Howes, S. Kille, Internet Engineering Task Force, RFC 2251

81. Lightweight Directory Access Protocol (v3) Extension for Transport Layer Security, J. Hodges, R. Morgan, M. Wahl, Internet Engineering Task Force, RFC 2830

82. Real Time Streaming Protocol (RTSP), H. Schulzrinne, A. Rao, M. Lanphier, Internet Engineering Task Force, RFC 2326

83. The Transport Layer Security (TLS) Protocol Version 1.1, T. Dierks, E. Rescola, Internet Engineering Task Force, RFC 4346

84. Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0, Organization for the Advancement of Structured Information Standards (OASIS), saml-core-2.0-os

85. Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, S. Chokani et al., Internet Engineering Task Force, RFC 3647

86. Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP), J. Peterson, C. Jennings, Internet Engineering Task Force, RFC 4474

87. eXtensible Access Control Markup Language (XACML) Version 2.0, Organization for the Advancement of Structured Information Standards (OASIS), XACML 2.0

88. The Secure Hash Algorithm, Federal Information Processing Standards Publication 180-2, National Institute of Standards and Technology, FIPS-PUB-180-2

89. Advanced Encryption Standard, Federal Information Processing Standards Publication 197, National Institute of Standards and Technology, FIPS-PUB-197

90. (Extensible Markup Language) XML-Signature Syntax and Processing, D. Eastlake, J. Reagle, D. Solo, Internet Engineering Task Force, RFC 3275

91. Simple Network Management Protocol, Version 3 (SNMPv3), J. Case et al., Internet Engineering Task Force, RFC 3410 through RFC 3418

92. RTP Control Protocol Extended Reports (RTCP XR), T. Friedman ed., Internet Engineering Task Force. RFC 3611

93. XML Path Language (XPath) Version 1.0, J. Clark, S. Derose, World Wide Web Consortium (W3C), TR/1999/REC-xpath-19991116

94. Common Alerting Protocol V1.0, A. Botterell, Organization for the Advancement of Structured Information Standards (OASIS), oasis-200402-cap-core-1.0

95. Emergency Provider Access Directory (EPAD) Technical Implementation Guide, J. Rowland, J. Lawton, COMCARE, EPAD TIG

96. Security Requirements for Cryptographic Modules, Federal Information Processing Standards Publication 140-3, National Institute of Standards and Technology, FIPS-PUB-140-3

97. Report from the Special Joint LTD/PONGI Tech/Ops team on Congestion Control in NG9-1-1 Technical Information Document, National Emergency Number Association, work in progress

98. An INVITE-Initiated Dialog Event Package for the Session Initiation Protocol (SIP), J. Rosenberg, H. Schulzrinne, R. Mahy, Internet Engineering Task Force, RFC 4235

99. 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

100. NENA Functional and Interface Standards for Next Generation 9-1-1 Version 1.0 (i3), National Emergency Number Association, NENA 08-002

101. NENA Technical Information Document Network/System Access Security, National Emergency Number Association, NENA 04-503

102. Filtering Location Notifications in the Session Initiation Protocol (SIP), R. Mahy, B. Rosen, H. Tschofenig, RFC 6447

103. Use of Device Identity in HTTP-Enabled Location Delivery (HELD) J. Winterbottom, M. Thomson, H. Tschofenig, R. Barnes, RFC 6155

104. NG9-1-1 Additional Data, National Emergency Number Association, NENA 71-001

105. Domain Names -- Concepts And Facilities, P. Mockapetris, RFC 1034

106. A DNS RR for specifying the location of services (DNS SRV), A. Gulbrandsen, P. Vixie, L. Esibov, RFC 2782

107. SIPconnect Technical Recommendation V1.0, C. Sibley, C. Gatch, SIPforum, sf-adopted-twg-IP_PBX_SP_Interop-sibley-sipconnect
108. NENA Next Generation United States Civic Location Data Exchange Format (CLDXF), NENA-STA-004.1-2014, National Emergency Number Association.
109. Managing Client-Initiated Connections in the Session Initiation Protocol (SIP), C. Jennings, R. Mahy, F. Audet et al., Internet Engineering Task Force, RFC 5626
110. Emergency Data Exchange Language Distribution Element (EDXL-DE) 1.0, M. Raymond, S. Webb, P. Aymond, Organization for the Advancement of Structured Information Standards, OASIS EDXL-DE v1.0
111. Synchronizing Service Boundaries and <mapping> Elements Based on the Location-to-Service Translation (LoST) Protocol, H. Schulzrinne, H. Tschofenig, RFC 6739
112. Session Initiation Protocol (SIP) Event Notification Extension for Notification Rate Control, A. Niemi, K. Kiss, S. Loreto, RFC 6446
113. Design Considerations for Session Initiation Protocol (SIP) Overload Control, V. Hilt, E. Noel, C. Shen, A. Abdelai, RFC 6357
114. XML Schema Part 2: Datatypes Second Edition, P. Biron, A. Malhotra, W3C, http://www.w3.org/TR/xmlschema-2/
115. Session Traversal Utilities for NAT (STUN), J. Rosenberg, R. Mahy, P. Matthews, D. Wing, Internet Engineering Task Force, RFC 5389
116. Framework for Real-Time Text over IP Using the Session Initiation Protocol (SIP), A. van Wijk, G. Gybels, Internet Engineering Task Force, RFC 5194
117. RTP Payload for Text Conversation, G. Hellstrom, P. Jones, Internet Engineering Task Force, RFC 4103
118. Framework for Transcoding with the Session Initiation Protocol (SIP), G. Camarillo, Internet Engineering Task Force, RFC 5369
119. Indication of Message Composition for Instant Messaging, H. Schulzrinne, Internet Engineering Task Force, RFC 3994
120. The Message Session Relay Protocol (MSRP), B. Campbell, R. Mahy, C. Jennings, Internet Engineering Task Force, RFC 4975
121. Relay Extensions for the Message Session Relay Protocol (MSRP), C. Jennings, R. Mahy, A.B. Roach, Internet Engineering Task Force, RFC 4976
122. Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types, N. Freed, N. Borenstein, Internet Engineering Task Force, RFC 2046
123. vCard Format Specification, S. Perreault, Internet Engineering Task Force, RFC 6350
124. The Secure Real-time Transport Protocol (SRTP), M. Baugher et al., Internet Engineering Task Force, RFC 3711
125. Session Description Protocol (SDP) Security Descriptions for Media Streams, F. Andreasen, M. Baugher, D. Wing, Internet Engineering Task Force, RFC 4568

126. Signalling System Number 7 (SS7) – Operator Services Network Capabilities, Alliance for Telecommunications Industry Solutions, ATIS-1000666.1999 (R2014).
127. An Extensible Markup Language (XML)-Based Format for Event Notification Filters, H. Khartabil, E. Leppanen, M. Lonnfors, J. Costa-Requena, Internet Engineering Task Force, RFC 4661
128. Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols, J. Rosenberg, Internet Engineering Task Force, RFC 5245
129. OGC Web Feature Service Implementation Specification Version 1.1.0, P. Vretanos, Open Geospatial Consortium, OGC04-094
130. OWS 7 Engineering Report – Geosynchronization service, P. Vretanos, Open Geospatial Consortium, OGC 10-069r2,Vretanos, Open Geospatial Consortium, OGC 10-069r2,
131. The Atom Syndication Format, M. Nottingham, R. Sayre, Internet Engineering Task Force, RFC 4287
132. The ATOM Publishing Protocol, J. Gregorio, B. de hOra, Internet Engineering Task Force, RFC 5023
133. Voice Extensible Markup Language (VoiceXML) Version 2.0, S. McGlashan et al., World Wide Web Consortium, REC-voicexml20-20040316
134. Real Time Streaming Protocol (RTSP), H. Schulzrinne, A. Rao, R. Lanphier, Internet Engineering Task Force, RFC 2326
135. The Session Description Protocol (SDP) Label Attribute, O. Levin, G. Camarillo, Internet Engineering Task Force, RFC 4574
136. An Extension to the Session Description Protocol (SDP) and Real-time Transport Protocol (RTP) for Media Loopback, H. Kaplan et al., Internet Engineering Task Force, RFC 6849
137. "Enhanced Variable Rate Codec, Speech Service Option 3 for Wideband Spread Spectrum Digital Systems", 3GPP2 TSGC-CC.S0014-A V1.0, TIA/EIA/IS-27-A; and also "RTP Payload Format for Enhanced Variable Rate Codecs (EVRC) and Selectable Mode Vocoders (SMV)", A. Li, RFC 3558.
138. "Enhanced Variable Rate Codec, Speech Service Option 3 and 68 for Wideband Spread Spectrum Digital Systems", 3GPP2 TSGC-C C.S0014-B V1.0, TIA/EIA/IS-127-B; and also "Enhancements to RTP Payload Formats for EVRC Family Codecs", Q. Xie, R. Kapoor, RFC 4788.
139. "Enhanced Variable Rate Codec, Speech Service Options 3, 68, and 70 for Wideband Spread Spectrum Digital Systems", 3GPP2 TSGC-C C.S0014-C V1.0, TIA/EIA/IS-127-C; and also "RTP Payload Format for the Enhanced Variable Rate Wideband Codec (EVRC-WB) and the Media Subtype Updates for EVRC-B Codec", H. Desineni, Q. Xie, RFC 5188.
140. "Enhanced Variable Rate Codec, Speech Service Options 3, 68, 70, and 73 for Wideband Spread Spectrum Digital Systems" 3GPP2 TSGC-C C.S0014-D V1.0 TIA/EIA/IS-127-D; and also "RTP payload format for Enhanced Variable Rate Narrowband-Wideband Codec(EVRC-NW)", RFC 6884

141. "NG Partner Program 9-1-1 Funding Report", NENA, NG Funding Report
142. "Next Generation 9-1-1 Transition Policy Implementation Handbook: A Guide for Identifying and Implementing Policies to Enable NG9-1-1", NENA, NG911 Transition Policy Handbook
143. "Additional Data related to a Call for Emergency Call Purposes", R. Gellens et al., Internet Engineering Task Force, draft-ietf-ecrit-additional-data (work in progress)
144. "RObust Header Compression (ROHC): Framework and four profiles: RTP, UDP, ESP, and uncompressed", C. Bormann et al., Internet Engineering Task Force, RFC 3095
145. "Geolocation Policy: A Document Format for Expressing Privacy Preferences for Location Information", H. Schulzrinne, H. Tschofenig et al, Internet Engineering Task Force, RFC 6772
146. "Common Policy: A Document Format for Expressing Privacy Preferences", H. Schulzrinne et al., Internet Engineering Task Force, RFC 4745
147. "Guide to Storage Encryption Technologies for End User Devices", K. Scarf one, M. Souppaya, M. Sexton, National Institute of Standards and Technology, NIST Special Publication 800-111
148. Emergency Incident Data Document, National Emergency Number Association, NENA/APCO-INF-005
149. URN Syntax, R. Moats, Internet Engineering Task Force, RFC 2141
150. xCard: vCard XML Representation, S. Perreault, Internet Engineering Task Force, RFC 6351
151. Legacy Selective Router Gateway Technical Standard, National Emergency Number Association, NENA-STA-XXX (work in progress)
152. Specifying Civic Address Extensions in the Presence Information Data Format Location Object (PIDF-LO), J. Winterbottom, et al., Internet Engineering Task Force, RFC 6848
153. Session Recording Protocol, L. Portman et al., Internet Engineering Task Force, draft-ietf-siprec-protocol (work in progress)
154. Session Initiation Protocol (SIP) Recording Metadata, R. Mohan, P. Ravindran, P. Kyzivat, Internet Engineering Task Force, draft-ietf-siprec-metadata (work in progress)
155. DNS Security Introduction and Requirements, R. Arends et al., Internet Engineering Task Force, RFC 4035
156. Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN), R. Mahy, P. Matthews, J. Rosenberg, Internet Engineering Task Force, RFC 5766
157. The international public telecommunication numbering plan, International Telecommunications Union, Recommendation E.164 (10/11)
158. Codec Control Messages in the RTP Audio-Visual Profile with Feedback (AVPF), S. Wenger, U. Chandra, B. Burman, Internet Engineering Task Force, RFC 5104
159. XML Schema for Media Control, O. Levin, R. Even, P. Hagendorf, RFC 5168
160. Multi-party Chat Using the Message Session Relay Protocol (MSRP), A. Niemi, M. Garcia-Martin, G. Sandbakken, Internet Engineering Task Force, RFC 7701

161. Extended RTP Profile for Real-time Transport Control Protocol (RTCP)-Based Feedback (RTP/AVPF), J. Ott et al., Internet Engineering Task Force, RFC 4585
162. Call Processing Language (CPL): A Language for User Control of Internet Telephony Services, J. Lennox, X. Wu and H. Schulzrinne, Internet Engineering Task Force, RFC 3880
163. Uniform Resource Identifier (URI): Generic Syntax, T. Berners-Lee, R. Fielding, L. Masinter, Internet Engineering Task Force, RFC 3986
164. Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0, Organization for the Advancement of Structured Information Standards (OASIS), saml-bindings-2.0-os
165. Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0, Organization for the Advancement of Structured Information Standards (OASIS), saml-profiles-2.0-os
166. Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0, Organization for the Advancement of Structured Information Standards (OASIS), saml-metadata-2.0-os
167. Interworking between Session Initiation Protocol (SIP) and Bearer Independent Call Control or ISDN User Part, Alliance for Telecommunications Industry Solutions, ATIS 1000679.2015
168. Discovering Location-to-Service Translation (LoST) Servers Using the Dynamic Host Configuration Protocol (DHCP), H. Schulzrinne et al., Internet Engineering Task Force, RFC 5223
169. Content-ID and Message-ID Uniform Resource Locators, E. Levinson, Internet Engineering Task Force, RFC 2392
170. Simple Mail Transfer Protocol, J. Klensin, Internet Engineering Task Force, RFC 5321
171. An Architecture for Differentiated Services, S. Blale, et. al., Internet Engineering Task Force, RFC 2475
172. Internet Calendaring and Scheduling Core Object Specification (iCalendar), B. Desruisseaux, Ed., Internet Engineering Task Force, RFC 5545
173. ECS – Connection and Ring Back Addendum [Supplement to ATIS-1000628.2000 (R2010)], Alliance For Telecommunications Industry Solutions, ATIS- 1000678.a.2001 (R2010).
174. Residential SIP Telephony Feature Specification, PacketCable™, PKT-SP-RSTF-109-120412, April 12, 2012
175. CMS to CMS Signaling, PacketCable™, PKT-SP-CMSS1.5-I07-120412, April 12, 2012
176. Integrated Services Digital Network (ISDN) User Part (ISUP) to Session Initiation Protocol (SIP) Mapping, G. Camarillo, et.al., Internet Engineering Task Force, RFC 3398
177. Definition of Events for Channel-Oriented Telephony Signalling, H. Schulzrinne, et.al., Internet Engineering Task Force, RFC 5244
178. Public Safety Answering Point (PSAP) Callback, H. Schulzrinne, H. Tschofenig, C. Holmberg, M. Patel, Internet Engineering Task Force, RFC 7090
179. RTP Payload for DTMF Digits, Telephony Tones, and Telephony Signals, H. Schulzrinne, et.al., Internet Engineering Task Force, RFC 4733
180. GR-246-CORE, Telcordia Technologies Specification of Signalling System Number 7



One Nation 9-1-1 One Number

181. The Directory: Public-key and attribute certificate frameworks, International Telecommunications Union, Recommendation X.509 (11/2008)

182. Representation of Uncertainty and Confidence in the Presence Information Data Format Location Object (PIDF-LO), M. Thomson, J. Winterbottom, Internet Engineering Task Force, RFC7459

183. Dynamic Extensions to the Presence Information Data Format Location Object (PIDF-LO), H. Schulzrinne et al., Internet Engineering Task Force, RFC5692

184. Dynamic Host Configuration Protocol, R. Droms, Internet Engineering Task Force, RFC 2131

185. SOAP Version 1.2 Part 1: Messaging Framework (Second Edition), M. Gugin et al., World Wide Web Consortium (W3C), TR/2007/REC-soap12-part1-20070427

186. Session Initiation Protocol (SIP) INFO Method and Package Framework, C. Holmberg, E. Burger, H. Kaplan, Internet Engineering Task Force, RFC 6086

187. Obtaining and Using Globally Routable User Agent URIs (GRUUs) in the Session Initiation Protocol (SIP), J. Rosenberg, Internet Engineering Task Force, RFC 5627

188. Candidate APCO NENA 2.105.1-201x NG9-1-1 Emergency Incident Data Document (EIDD)

189. The tel URI for Telephone Numbers, H. Schulzrinne, Network Working Group, Internet Engineering Task Force, RFC 3966

190. ATIS Standard for Implementation of 3GPP Common IMS Emergency Procedures for IMS Origination and ESInet/Legacy Selective Router Termination, May, 2015. ATIS-0700015.v003.

191. 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.

192. HTTP over TLS, RFC 2818

193. Domain-Based Application Service Location Using URIs and the Dynamic Delegation Discovery Service (DDDS), RFC 4848

194. Discovering the Local Location Information Server (LIS), RFC 5986

195. A Session Initiation Protocol (SIP) Event Package for Key Press Stimulus (KPML), RFC 4730

196. Identification cards –Integrated circuit cards ISO/IEC 7816 (1-15)

197. Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1, RFC 3447

198. The HMAC-SHA-256-96 Algorithm and Its Use With IPsec, <draft-ietf-ipsec-ciph-sha-256-00.txt>

199. CCS/SS7 Generic Requirements in Support of E9-1-1 Service, GR-2956-CORE

200. LSSGR: Switching System Generic Requirements for Call Control Using the Integrated Services Digital Network User Part (ISDNUP), GR-256-CORE

201. Representing Trunk Groups in tel/sip Uniform Resource Identifiers (URIs), RFC 4904

202. Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing, RFC 7230

203. NENA Recommendation for the implementation of Enhanced MF Signaling, E9-1-1 Tandem to PSAP, NENA 03-002

204. Recommended Generic Standards for E9-1-1 PSAP Equipment, NENA 04-001

205. NENA ALI Query Service Standard, NENA 04-005

# 15 Previous Acknowledgments

NENA 08-003, Executive Board Approval Date, 06/14/2011

| **Members** | **Company** |
|---|---|
| Brian Rosen –Work Group Leader and Technical Editor | NeuStar |
| Nate Wilcox – VoIP/Packet Technical Chair | microDATA |
| Richard Atkins | Tarrant County 9-1-1 District |
| Delaine Arnold | Arnold 9-1-1 Consulting |
| Wayne Ballantyne | Motorola |
| Deborah Barclay | Alcatel Lucent |
| Marc Berryman | DDTI |
| Tom Breen | AT&T |
| Gary Brown | NENA Utah Chapter Member |
| Pete Eggimann | Metropolitan Emergency Services Board |
| Randall Gellens | Qualcomm Technologies, Inc, |
| Casimer M (Duke) Kaczmarczyk | Verizon |
| Marc Linsner | Cisco |
| Roger Marshall | TeleCommunication Systems, (TCS) |
| Kathy McMahon-Ruscitto | APCO International |
| Theresa Reese | Telcordia |
| Greg Schumacher | Sprint |
| Matthew Serra | Rave Mobile Safety (Smart911) |
| Robert Sherry | Intrado |
| Michael Smith | DSS |
| Hannes Tschofenig | Nokia Siemens Networks |
| Mike Vislocky | Network Orange |

# Appendix A – Mapping Data Elements between Legacy and NG9-1-1 (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 headers, PIDF-LO parameters or Additional Data Elements (**NENA 02-010 Field Name → PIDF-LO and/or Additional Data**) for use within the NG9-1-1 system. The LPG must map SIP headers, PIDF-LO parameters or Additional Data Elements to legacy elements (**PIDF-LO and/or Additional Data → NENA 02-010 Field Name**) for display in legacy PSAPs. The format of Table A-15-1 that is used in the "Standard ALI Query Best Practices" may be found on NENA.org.

A future revision 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)[72]<br>SIP INVITE/P-Preferred-Identity (P-P-I) for Non Service Initiated calls |
| CallingPartyNum (ANI) | SIP INVITE/P-Asserted-Identity (P-A-I) [61] |
| ClassOfService | Included in Additional Data and PIDF-LO. See Table A-15-2 |
| TypeOfService | See Table A-15-3 |
| SourceOfService | N/A |
| MainTelNum | EmergencyCallData:SubscriberInfo/vcards/vcard/tel[n]/uri=tel:uri with MainTelNum in +1 context<br>AND<br>EmergencyCallData:SubscriberInfo/vcards/vcard/tel[n]/parameters/type/text=main |
| CustomerName | EmergencyCallData:SubscriberInfo/vcards/vcard/fn/text |
| CustomerCode | N/A |
| AttentionIndicator | N/A |
| SpecialMessage | N/A |
| 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 |

[72] 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.

| **NENA AQS Element** | **NG9-1-1 Mapping** |
|---|---|
| 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]<br>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]<br>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<br><br>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<br><br>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 |
| ***Location Info: Geo Location*** | |
| Latitude | pidflo:presence/tuple/status/geopriv/location-info/Circle/gml:pos [latitude part]<br>OR<br>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]<br>OR<br>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 [183] Dynamic Host Configuration Protocol [184] |
| Speed (in KPH/MPH) | pidflo:presence/tuple/status/geopriv10:/location-info/Dynamic/speed |
| PositionSource | See Table A-15-4 and Table A-15-5 |
| Uncertainty | pidflo:presence/tuple/status/geopriv/location-info/Circle/radius<br>OR<br>pidflo:presence/tuple/status/geopriv/location-info/Sphere/radius uom="urn:ogc:def:uom:EPSG::9001" |

| NENA AQS Element | NG9-1-1 Mapping |
|---|---|
| Confidence | pidflo:presence/tuple/status/geopriv/location-info/confidence [182] |
| DateStamp<br>Represents the time of the location fix | pidflo:presence/tuple/timestamp<br>Represents the time the PIDF 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 (format carrier-specific) |
| SectorID | From SIP P-Access-Network-Info if passed (format carrier-specific) |
| LocationDescription | pidflo:presence/tuple/status/geopriv/location-info/civicAddress/LOC |
| ***Location Info*** | |
| Comment | EmergencyCallData:comment |
| ***Agencies:Police*** | From ECRF |
| Name | LoST:findServiceResponse/mapping/displayName<br>AND<br>LoST:findServiceResponse/mapping/service=urn:nena:service:responder.police |
| TN | LoST:findServiceResponse/mapping/uri=tel:uri with TN in +1 context |
| ***Agencies:Fire*** | From ECRF |
| Name | LoST:findServiceResponse/mapping/displayName<br>AND<br>LoST:findServiceResponse/mapping/service=urn:nena:service:responder.fire |
| TN | LoST:findServiceResponse/mapping/uri=tel:uri with TN in +1 context |
| ***Agencies:EMS*** | From ECRF |
| Name | LoST:findServiceResponse/mapping/displayName<br>AND<br>LoST:findServiceResponse/mapping/service=urn:nena:service:responder.ems |
| TN | LoST:findServiceResponse/mapping/uri=tel:uri with TN in +1 context |
| ***Agencies: OtherAgencies*** | From ECRF |
| Name | LoST:findServiceResponse/mapping/displayName<br>AND<br>LoST:findServiceResponse/mapping/service=urn:nena:service:responder.<br>“agency” (Replace agency with appropriate name.) |
| TN | LoST:findServiceResponse/mapping/uri=tel:uri with TN in +1 context |
| ***Agencies*** | |
| AdditionalInfo | N/A |
| ESN | Mapped from PIDF-LO via MCS |
| ***SourceInfo: DataProvider*** | |
| DataProviderID | EmergencyCallData.ProviderInfo/ProviderID |
| TN | EmergencyCallData.ProviderInfo/ContactURI in the form of a tel:uri [RFC 3966] [189] in E.164 format fully specified with country code |
| Name | EmergencyCallData.ProviderInfo/DataProviderString |
| | Type: EmergencyCallData.ProviderInfo/TypeOfProvider |
| ***SourceInfo: AccessProvider*** | Map when type is EmergencyCallData.ProviderInfo/TypeOfProvider=Access Network Provider |
| AccessProviderID | EmergencyCallData.ProviderInfo/ProviderID |

| NENA AQS Element | NG9-1-1 Mapping |
|---|---|
| TN | EmergencyCallData.ProviderInfo/ContactURI in the form of a tel:uri [RFC 3966] [189] in E.164 format fully specified with country code |
| Name | EmergencyCallData.ProviderInfo/DataProviderString |
| ***SourceInfo*** | |
| ALIUpdateGMT | N/A |
| ALIRetreivalGMT | 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-15-1 Data Element Mapping**

NOTE: A future revision of this document will describe how parameters in an AQS query are handled by NG9-1-1 elements.

| Legacy CoS Code | Legacy Value | NG9-1-1 Data Structure |
|---|---|---|
| 1 | Residence | pidflo:presence/tuple/status/geopriv/method=Manual<br>and<br>EmergencyCallData.ServiceInfo/ServiceType=POTS<br>and<br>EmergencyCallData.ServiceInfo/ServiceEnvironment=Residence<br>and<br>EmergencyCallData.ServiceInfo/ServiceMobility=Fixed |
| 2 | Business | pidflo:presence/tuple/status/geopriv/method=Manual<br>and<br>EmergencyCallData.ServiceInfo/ServiceType=POTS<br>and<br>EmergencyCallData.ServiceInfo/ServiceEnvironment=Business<br>and<br>EmergencyCallData.ServiceInfo/ServiceMobility=Fixed |
| 3 | Residence PBX | pidflo:presence/tuple/status/geopriv/method=Manual<br>and<br>EmergencyCallData.ServiceInfo/ServiceType=MLTS-local<br>and<br>EmergencyCallData.ServiceInfo/ServiceEnvironment=Residence<br>and<br>EmergencyCallData.ServiceInfo/ServiceMobility=Fixed |
| 4 | Business PBX | pidflo:presence/tuple/status/geopriv/method=Manual<br>and<br>EmergencyCallData.ServiceInfo/ServiceType=MLTS-local |

| Legacy CoS Code | Legacy Value | NG9-1-1 Data Structure |
|---|---|---|
| | | and<br>EmergencyCallData.ServiceInfo/ServiceEnvironment=Business<br>and<br>EmergencyCallData.ServiceInfo/ServiceMobility=Fixed |
| 5 | Centrex | pidflo:presence/tuple/status/geopriv/method=Manual<br>and<br>EmergencyCallData.ServiceInfo/ServiceType=MLTS-hosted<br>and<br>EmergencyCallData.ServiceInfo/ServiceEnvironment=Business<br>and<br>EmergencyCallData.ServiceInfo/ServiceMobility=Fixed |
| 6 | Coin 1 way out | pidflo:presence/tuple/status/geopriv/method=Manual<br>and<br>EmergencyCallData.ServiceInfo/ServiceType=coin;one-way<br>and<br>EmergencyCallData.ServiceInfo/ServiceEnvironment=Business<br>and<br>EmergencyCallData.ServiceInfo/ServiceMobility=Fixed |
| 7 | Coin 2 way | pidflo:presence/ tuple/status/geopriv/method=Manual<br>and<br>EmergencyCallData.ServiceInfo/ServiceType=coin<br>and<br>EmergencyCallData.ServiceInfo/ServiceEnvironment=Business<br>and<br>EmergencyCallData.ServiceInfo/ServiceMobility=Fixed |
| 8 | Wireless Phase 0 | pidflo:presence/tuple/status/geopriv/method=Manual<br>and<br>EmergencyCallData.ServiceInfo/ServiceType=wireless<br>and<br>EmergencyCallData.ServiceInfo/ServiceMobility =Mobile |
| 9 | Residence OPX | pidflo:presence/tuple/status/geopriv/method=Manual<br>and<br>EmergencyCallData.ServiceInfo/ServiceType=POTS;remote<br>and<br>EmergencyCallData.ServiceInfo/ServiceEnvironment=Residence<br>and<br>EmergencyCallData.ServiceInfo/ServiceMobility=Fixed |
| 0 | Business OPX | pidflo:presence/tuple/status/geopriv/method=Manual<br>and<br>EmergencyCallData.ServiceInfo/ServiceType=POTS;remote<br>and<br>EmergencyCallData.ServiceInfo/ServiceEnvironment=Business<br>and<br>EmergencyCallData.ServiceInfo/ServiceMobility=Fixed |
| A | Customer owned Coin | pidflo:presence/tuple/status/geopriv/method=Manual<br>and<br>EmergencyCallData.ServiceInfo/ServiceType=Coin<br>and<br>EmergencyCallData.ServiceInfo/ServiceEnvironment=Business |

| Legacy CoS Code | Legacy Value | NG9-1-1 Data Structure |
|---|---|---|
| | | and<br>EmergencyCallData.ServiceInfo/ServiceMobility=Fixed |
| B | Not Available | N/A |
| C | VoIP Residence | pidflo:presence/tuple/status/geopriv/method=Manual<br>and<br>EmergencyCallData.ServiceInfo/ServiceType=VOIP<br>and<br>EmergencyCallData.ServiceInfo/ServiceEnvironment=Residence<br>and<br>EmergencyCallData.ServiceInfo/ServiceMobility=Unknown |
| D | VoIP Business | pidflo:presence/tuple/status/geopriv/method=Manual<br>and<br>EmergencyCallData.ServiceInfo/ServiceType=VOIP<br>and<br>EmergencyCallData.ServiceInfo/ServiceEnvironment=Business<br>and<br>EmergencyCallData.ServiceInfo/ServiceMobility=Unknown |
| E | VoIP Coin or Pay Phone | pidflo:presence/tuple/status/geopriv/method=Manual<br>and<br>EmergencyCallData.ServiceInfo/ServiceType=VOIP;coin<br>and<br>EmergencyCallData.ServiceInfo/ServiceEnvironment=Business<br>and<br>EmergencyCallData.ServiceInfo/ServiceMobility=Unknown |
| F | VoIP Wireless | pidflo:presence/tuple/status/geopriv/method=Manual<br>and<br>EmergencyCallData.ServiceInfo/ServiceType=VOIP;wireless<br>and<br>EmergencyCallData.ServiceInfo/ServiceMobility=Mobile |
| J | VoIP Nomadic | pidflo:presence/tuple/status/geopriv/method=Manual<br>and<br>EmergencyCallData.ServiceInfo/ServiceType=VOIP<br>and<br>EmergencyCallData.ServiceInfo/ServiceMobility=Nomadic |
| K | VoIP Enterprise | pidflo:presence/tuple/status/geopriv/method=Manual<br>and<br>EmergencyCallData.ServiceInfo/ServiceType=VOIP<br>and<br>EmergencyCallData.ServiceInfo/ServiceEnvironment=Business<br>and<br>EmergencyCallData.ServiceInfo/ServiceMobility=Unknown |
| G | Wireless Phase I | pidflo:presence/tuple/status/geopriv/method=Cell<br>and<br>EmergencyCallData.ServiceInfo/ServiceType=wireless<br>and<br>EmergencyCallData.ServiceInfo/ServiceMobility=Mobile |
| H | Wireless Phase II | pidflo:presence/tuple/status/geopriv/method= (See Table A-15-4 and Table A-15-5 LTY to i3 Mapping)<br>and |



One Nation 9-1-1 One Number

| Legacy CoS Code | Legacy Value | NG9-1-1 Data Structure |
|---|---|---|
| | | EmergencyCallData.ServiceInfo/ServiceType=wireless<br>and<br>EmergencyCallData.ServiceInfo/ServiceMobility=Mobile |
| I | Wireless Phase II returning Phase I | pidflo:presence/tuple/status/geopriv/method=Cell<br>and<br>EmergencyCallData.ServiceInfo/ServiceType=wireless<br>and<br>EmergencyCallData.ServiceInfo/ServiceMobility=Mobile |
| V | Voice Over IP | pidflo:presence/tuple/status/geopriv/method=Manual<br>and<br>EmergencyCallData.ServiceInfo/ServiceType=VOIP<br>and<br>EmergencyCallData.ServiceInfo/ServiceMobility=Unknown |

**Table A-15-2 Class of Service Mapping**

| TYS Codes | TYS Values | NG9-1-1 Data Structure |
|---|---|---|
| 0 | Not FX nor Non-Published | Normal SIP header 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 |
| 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-15-3 Type of Service Mapping**

Clarifications on Table A-15-3: 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 | Unspecified | 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[73] |
| 4 | networkTDOA | pidflo:presence/tuple/status/geopriv/method= networkTDOA[63] |
| 5 | networkRFFingerprinting | pidflo:presence/tuple/status/geopriv/method= |

[73] Submit method to IANA Method Token Registry.

| Value | Name | PIDF-LO Mapping |
|---|---|---|
| | | networkRFFingerprinting[63] |
| 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 |
| 32 | hybridUnspecified | Method not included in PIDF-LO |
| 33 | hybridAGPS_AFLT | pidflo:presence/tuple/status/geopriv/method= hybridAGPS_AFLT[63] |
| 34 | hybridCellSector_AGPS | pidflo:presence/tuple/status/geopriv/method= hybridCellSector_AGPS[63] |
| 35 | hybridNetworkTDOA_AOA | pidflo:presence/tuple/status/geopriv/method= hybridNetworkTDOA_AOA[63] |
| 36 | hybridNetworkTDOA_AGPS | pidflo:presence/tuple/status/geopriv/method= hybridNetworkTDOA_AGPS[63] |
| 37 | hybridTDOA_AGPS_AOS | pidflo:presence/tuple/status/geopriv/method= hybridTDOA_AGPS_AOS[63] |
| 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 |
| 50 | cosWPH1 | pidflo:presence/tuple/status/geopriv/method=Cell |
| 51 | cosWPH2 | Method not included in PIDF-LO |

**Table A-15-4 LNG Mapping for Position Source – E2 to PIDF-LO**

| 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[63] |
| A-GNSS | pidflo:presence/tuple/status/geopriv/method=A-GNSS[63] |
| 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[63] |
| UNKNOWN | Method not included in PIDF-LO |
| OTHER | Method not included in PIDF-LO |

**Table A-15-5 LNG Mapping for Position Method – MLP to PIDF-LO**

# Appendix B – SI Provisioning Data Model

The Model below is for use in the interface between the SI and the ECRF/LVF. It may not represent data actually stored in the GIS system. The SI would convert from the internal format to this format.

The USE M/C is an indication that the field is Mandatory or Conditional in a record. All fields must be implemented. If the field is Mandatory, the individual attribute information in the field may be blank if they are not present.

Attribute names and descriptions are drawn from CLDXF [108] where appropriate. Any difference between the definition of fields other than right/left and similar modifications between this model and CLDXF are resolved in favor of the CLDXF definition.

Non-authoritative data must not be sent to an ECRF/LVF over the SI.

Note: Additional fields to allow MSAG Conversion Service to operate correctly must be added. Definition of applicable MSAG data fields is a priority for i3v3.

## B.1 Centerlines

| ATTRIBUTE NAME | USE M/C | TYPE | DATA DESCRIPTION |
|---|---|---|---|
| Source of Data | M | A | Agency that last updated the record – usually the name of the 9-1-1 Authority |
| Data Updated | M | AN | Date of last update as a Timestamp |
| Effective Date | C | AN | Date the new information goes into effect as a Timestamp |
| Expiration Date | C | AN | Date this feature is no longer effective using as a Timestamp |
| Unique ID | M | AN | Unique ID for each Road Segment, with domain of agency included. ID's not to be re-used when road is split or deleted. Ex. 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. Ex. US (country in RFC 5139) [76] |
| 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. Ex. US (country in RFC 5139) [76] |
| State Left | M | A | The name of a state, province or equivalent on the left side of where the road is located, |

| ATTRIBUTE NAME | USE M/C | TYPE | DATA DESCRIPTION |
|---|---|---|---|
| | | | as specified in CLDXF or its Canadian equivalent.<br>Ex. TX (A1 in RFC 5139) [76] |
| 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.<br>Ex. TX (A1 in RFC 5139) [76] |
| County Left[1] | M | AN | 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.<br>Ex. Harris (A2 in RFC 5139) [76] |
| County Right[1] | M | AN | 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.<br>Ex. Harris (A2 in RFC 5139) [76] |
| AddionalCodeLeft | C | AN | 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 |
| AdditionalCodeRight | C | AN | 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 |
| Incorporated Municipality Left | M | A | 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. Only used if a named incorporated municipality exists, otherwise populate with “Unincorporated”.<br>Ex. Chicago (A3 in RFC 5139) |
| Incorporated Municipality Right | M | A | The name of the incorporated municipality or other general-purpose local governmental unit (if any) on the right side of where the |

| ATTRIBUTE NAME | USE M/C | TYPE | DATA DESCRIPTION |
|---|---|---|---|
| | | | road is located, as specified in CLDXF or its Canadian equivalent. Only used if a named incorporated municipality exists, otherwise populate with "Unincorporated".<br>Ex. Chicago (A3 in RFC 5139) [76] |
| Unincorporated Community Right | C | A | 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) [76] |
| Unincorporated Community Left | C | A | 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) [76] |
| Neighborhood Community Right | C | A | 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) [76] |
| Neighborhood Community Left | C | A | 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) [76] |
| Street Segment | M | S | StreetSegment |
| Alias Street Segment | C | S | StreetSegment, may occur more than once |
| Road Class | M | A | Primary, Secondary, Local, Ramp, Service, Vehicular Trail, Walkway, Alley, Private, Parking Lot, Trail, Other as specified in MAF/TIGER Feature Classification Codes (MTFCC) Attachment D, series S |
| One-way | C | A | One-way road classification<br>• B or blank – travel in both directions<br>• FT – One-way from FROM node to TO node (in direction of arc);<br>• TF – One way from TO node to FROM Node (opposite direction of arc) |
| Speed Limit | C | N | Normal Posted Speed in mph |
| Postal Community Name Left | M | 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)[76] |

| ATTRIBUTE NAME | USE M/C | TYPE | DATA DESCRIPTION |
|---|---|---|---|
| Postal Community Name Right | M | 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) [76] equivalent |
| Postal Code Left | M | AN | Postal Code, on the left side of where the road is located, as specified in CLDXF or its Canadian equivalent (PC in RFC 5139) [76] |
| Postal Code Right | M | AN | Postal Code on the right side of where the road is located, as specified in CLDXF or its Canadian equivalent[3] (PC in RFC 5139) [76] |
| ESN Left | C | AN | 3-5 digit Emergency Service Number associated with the Left side of the street[3] |
| ESN Right | C | AN | 3-5 digit Emergency Service Number associated with the Right side of the street[3] |

## B.2 Street/Address Structures

### B.2.1 CompleteStreetName

| ATTRIBUTE NAME | USE M/C | TYPE | DATA DESCRIPTION |
|---|---|---|---|
| Street Name Pre Modifier | C | A | A street pre-modifier as specified in CLDXF or its Canadian equivalent. (PRM in RFC 5139) [76]. Examples: Alternate, Business, Bypass, Extended, Historic, Loop, Old, Private, Public, Spur, etc. |
| Street Name Pre Directional | C | A | A street name pre-directional as specified in CLDXF or its Canadian equivalent (PRD in RFC 5139) [76] |
| Street Name Pre Type | C | A | A street name pre-type as specified in CLDXF or its Canadian equivalent (STP in RFC 6848) [152] |
| Street Name Pre Type Separator | C | A | 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 | C | A | The street name as specified in CLDXF or its Canadian equivalent. Required unless there is a Complete Landmark Name and no Street Name available. (RD in RFC 5139) [76] |

| ATTRIBUTE NAME | USE M/C | TYPE | DATA DESCRIPTION |
|---|---|---|---|
| Street Name Post Type | C | A | The street name post type as specified in CLDXF or its Canadian equivalent. (STS in RFC 5139) [76] |
| Street Name Post Directional | C | A | The street name post directional as specified in CLDXF or its Canadian equivalent (POD in RFC 5139) [76] |
| Street Name Post Modifier | C | A | The street name post modifier as specified in CLDXF or its Canadian equivalent. (POM in RFC 5139) [76]. 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 | TYPE | DATA DESCRIPTION |
|---|---|---|---|
| Address Number Prefix | C | AN | The address number prefix as specified in CLDXF or its Canadian equivalent (HNP in RFC 6848) [152] |
| Address Number | M | N | The Address Number as specified in CLDXF or its Canadian equivalent. (HNO in RFC 5139) [76] |
| Address Number Suffix | C | AN | The Address Number Suffix as specified in CLDXF or its Canadian equivalent. |

### B.2.3 StreetSegment

| ATTRIBUTE NAME | USE M/C | TYPE | DATA DESCRIPTION |
|---|---|---|---|
| Complete Street Name | M | S | CompleteStreetName |
| Left Address Number Prefix | C | A | 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 FROM Node" of the arc segment. It is quite possible that this address be higher than the "Left TO Node" ex. 399 |
| 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 TO Node" of the arc segment. It is quite possible |

| ATTRIBUTE NAME | USE M/C | TYPE | DATA DESCRIPTION |
|---|---|---|---|
| | | | that this address be lower than the "Left From Address" ex. 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 | C | A | 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 | C | 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 | C | A | 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 | R | A | Like Parity Left, but applying to the right side of the road. |
| Right Address Number Suffix | C | A | Like Left Address Number Suffix, but applying to the right side of the road. |
| Validation Right | C | A | Like Validation Left, but applying to the right side of the road. 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. |

### B.2.4 CompleteAddress

| ATTRIBUTE NAME | USE M/C | TYPE | DATA DESCRIPTION |
|---|---|---|---|
| Complete Street Name | M | S | CompleteStreetName |
| Complete Address Number | M | S | CompleteAddressNumber |
| Milepost | C | A | Milepost as specified in CLDXF or its Canadian equivalent (MP in RFC 6848) [152] |

## B.3 Site/Structure

| ATTRIBUTE NAME | USE M/C | TYPE | DATA DESCRIPTION |
|---|---|---|---|

| ATTRIBUTE NAME | USE M/C | TYPE | DATA DESCRIPTION |
|---|---|---|---|
| Source of Data | M | A | Agency that last updated the record – Agency ID e.g., the domain name of the 9-1-1 Authority |
| Date Updated | M | AN | Date of last as a Timestamp |
| Effective Date | C | AN | Date the new layer information goes into effect, as a Timestamp |
| Expiration Date | C | AN | Date this feature is no longer effective, as a Timestamp |
| Unique_ID | M | AN | 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. |
| State | M | A | The 2-character abbreviation of a state, province or equivalent, as specified in CLDXF or its Canadian equivalent. ex. TX (A1 in RFC 5139) [76] |
| County[1] | M | A | The name of county or county-equivalent as described in CLDXF or its Canadian equivalent [2] (A2 in RFC 5139) [76] |
| AdditionalCode | C | A | 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 | C | R | The name of the incorporated municipality or other general-purpose local governmental unit as specified in CLDXF or its Canadian equivalent [4]. Specify "unincorporated" or "unknown" if necessary. (A3 in RFC 5139) [76] |
| Unincorporated Community | C | A | The name of an unincorporated community, division, or area, as specified in CLDXF or its Canadian equivalent (A4 in RFC 5139) [76] |
| Neighborhood Community | C | A | The name of an unincorporated neighborhood, subdivision or area, as specified in CLDXF or its Canadian equivalent. (A5 in RFC 5139) [76] |
| Address | M | S | CompleteAddress |
| Alias Address | C | S | CompleteAddress. May occur more than once. |

| ATTRIBUTE NAME | USE M/C | TYPE | DATA DESCRIPTION |
|---|---|---|---|
| ESN[4] | C | AN | Emergency Service Number associated with this House Number, Street Name and Community Name[3] |
| Postal Community Name | M | 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) [76] |
| Postal Code | M | AN | Postal code ex. 05421 Format: ANANAN (PC in RFC 5139) [76] |
| Building | C | AN | The name of a building as specified in CLDXF or its Canadian equivalent. Examples: DuPont Hotel, Shiloh Church, Tower B (BLD in RFC 5139) [76] |
| Floor | C | AN | A floor, story, or level within a building as specified in CLDXF or its Canadian equivalent (FLR in RFC 5139) [76] |
| Unit | C | AN | 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. Examples: Apartment 101, Suite 233-A (UNIT in RFC 5139) [76] |
| Room | C | AN | A single room within a building or unit as specified in CLDXF or its Canadian equivalent. Examples: Bedroom, Exam Room 3, Ballroom (ROOM in RFC 5139) [76] |
| Seat | C | AN | A place where a person might sit within a room as specified in CLDXF or its Canadian equivalent. Example Seat 35A, Cubicle 1A213 (SEAT in RFC 5139) [76] |
| CompleteLandmarkName | C | AN | The complete name by which a prominent feature is publicly known as specified in CLDXF or its Canadian equivalent (LMK in RFC 5139) [76] |
| LandmarkNamePart | C | AN | 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) |
| Additional Location Information | C | AN | 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) [76] |
| Place-Type | M | A | Type of place, e.g., office, store, school, |

| ATTRIBUTE NAME | USE M/C | TYPE | DATA DESCRIPTION |
|---|---|---|---|
| | | | residential as specified in CLDXF or its Canadian equivalent (PLC in RFC 5139) [76] |
| AdditionalDataURI | C | URI | URI of Additional Data for this site/structure. May occur more than once. |

Notes:

[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 FIPS Codes Standard shall not apply to applications involving interchange of international data that require the use of the country codes of the International Organization for Standardization, i.e., ISO 3166. For the convenience of such users, the ISO 3166 country codes are published in FIPS PUB 104, *Guideline for Implementation of ANSI Codes for the Representation of Names of Countries, Dependencies, and Areas of Special Sovereignty*. FIPS PUB 104 provides both two- and three-character alphabetic codes for each entity listed. Federal agencies that do not require FIPS PUB 104 for international data interchange, and are not involved in national defense programs or with the mission of the U.S. Department of State, may adopt either set of codes. (See http://wwww.ntis.gov/products/ntrl)

[3] 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.

[4] Used in Legacy Systems and is not used in a full i3 implementation

[5] Setting Validation Flag to SSVAL will result in the House Number (HNO) being validated against the Site Structure location layer. If the House Number is not valid in the Site Structure Layer, the HNO field will have either a <valid> or <invalid> response from the LVF.

[6] Setting the Validation Flag to SSNR will result in the HNO being first checked against the Site/Structure layer, and if there is no Site/Structure with that House Number, a range validation will be performed against the Left/Right range values in Road Centerline. If the House Number is within a range of values of the appropriate Road Center Line, the LVF will return "unchecked". If the House Number is not within a range, the LVF will return "invalid".

[7]If the subaddress validation flags are not specified, they default to U if data is not provisioned in the LVF for the field, and R if data is provisioned.

All of these fields may not be loaded into the ECRF.

These are the minimum data, there can be many other fields not shown e.g., direction of travel, number of lanes.

All other existing GIS data layer schemas, other than the revised layers shown above, should be used.

## B.4 State Boundary

| ATTRIBUTE NAME | USE M/C | TYPE | DATA DESCRIPTION |
|---|---|---|---|
| Source of Data | M | A | Agency that last updated the record – Agency ID e.g., the domain name of the 9-1-1 Authority |
| Date Updated | M | AN | Date of last update as a Timestamp |
| Effective Date | C | AN | Date the new layer information goes into effect as a Timestamp |
| Expiration Date | C | AN | Date this feature is no longer effective as a Timestamp |
| Unique_ID | M | AN | Unique ID for each record |
| Country | M | A | The name of a country represented by its |

| ATTRIBUTE NAME | USE M/C | TYPE | DATA DESCRIPTION |
|---|---|---|---|
| | | | two-letter ISO 3166-1 English country alpha-2 code elements in capital ASCII letters, as specified in CLDXF or its Canadian equivalent. |
| State | M | A | The name of a state, province or equivalent, as specified in CLDXF or its Canadian equivalent. ex. TX (A1 in RFC 5139) [76] |

## B.5 County Boundary

| ATTRIBUTE NAME | USE M/C | TYPE | DATA DESCRIPTION |
|---|---|---|---|
| Source of Data | M | A | Agency that last updated the record – Agency ID e.g., the domain name of the 9-1-1 Authority |
| Date Updated | M | A | Date of last update as a Timestamp |
| Date | C | AN | Date of last update as a Timestamp |
| Effective Date | C | AN | Date the new layer information goes into effect as a Timestamp |
| Expiration Date | C | AN | Date this feature is no longer effective as a Timestamp |
| Unique_ID | M | AN | 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. |
| State | M | A | The name of a state, province or equivalent, as specified in CLDXF or its Canadian equivalent. ex. TX (A1 in RFC 5139) [76] |
| County | C | A | The name of county or county-equivalent as specified in CLDXF or its Canadian equivalent [1]. (A2 in RFC 5139) [76] |

## B.6 Incorporated Municipality Boundary

| ATTRIBUTE NAME | USE M/C | TYPE | DATA DESCRIPTION |
|---|---|---|---|
| Source of Data | M | A | Agency that last updated the record – Agency ID e.g., the domain name of the 9-1-1 Authority |
| Date Updated | M | AN | Date of last update as a Timestamp |
| Effective Date | C | AN | Date the new layer information goes into effect as a Timestamp |
| Expiration Date | C | AN | Date this feature is no longer effective as a Timestamp |

| ATTRIBUTE NAME | USE M/C | TYPE | DATA DESCRIPTION |
|---|---|---|---|
| Unique_ID | M | AN | Unique ID for each record |
| Country | M | AN | The name of a country represented by its two-letter ISO 3166-1 English country alpha-2 code elements in capital ASCII letters. |
| State | M | A | The name of a state, province or equivalent as specified in CLDXF or its Canadian equivalent. Example: TX (A1 in RFC 5139) [76] |
| County | C | A | The name of county or county-equivalent as specified in CLDXF or its Canadian equivalent[1]. (A2 in RFC 5139) [76] |
| AddtionalCode | C | A | 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 | M | A | The name of the incorporated municipality or other general-purpose local governmental unit as specified in CLDXF or its Canadian equivalent (A3 in RFC 5139) [76] |

## B.7 Unincorporated Community Boundary

| ATTRIBUTE NAME | USE M/C | TYPE | DATA DESCRIPTION |
|---|---|---|---|
| Source of Data | M | A | Agency that last updated the record – Agency ID e.g., the domain name of the 9-1-1 Authority |
| Date Updated | M | AN | Date of last update as a Timestamp |
| Effective Date | C | AN | Date the new layer information goes into effect, as a Timestamp |
| Expiration Date | C | AN | Date this feature is no longer effective, as a Timestamp |
| Unique_ID | M | AN | Unique ID for each record |
| Country | M | AN | The name of a country represented by its two-letter ISO 3166-1 English country alpha-2 code elements in capital ASCII letters. |
| State | M | A | The name of a state, province or equivalent, as specified in CLDXF or its Canadian equivalent. Example: TX (A1 in RFC 5139) [76] |
| County | C | A | The name of county or county-equivalent as specified in CLDXF or its Canadian |

| ATTRIBUTE NAME | USE M/C | TYPE | DATA DESCRIPTION |
|---|---|---|---|
| | | | equivalent [1]. (A2 in RFC 5139) [76] |
| AdditionalCode | C | A | 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 | C | A | The name of the incorporated municipality or other general-purpose local governmental unit as specified in CLDXF or its Canadian equivalent. Specify "unincorporated" or "unknown" if necessary. (A3 in RFC 5139) [76] |
| Unincorporated Community | M | A | The name of an unincorporated community, as specified in CLDXF or its Canadian equivalent (A4 in RFC 5139) [76]. |

## B.8 Service Boundary

| ATTRIBUTE NAME | USE M/C | TYPE | DATA DESCRIPTION |
|---|---|---|---|
| Source of Data | M | A | Agency that last updated the record – Agency ID e.g., the domain name of the 9-1-1 Authority |
| Date Updated | M | AN | Date of last update as a Timestamp |
| Effective Date | C | AN | Date the new layer information goes into effect, as a Timestamp |
| Expiration Date | C | AN | Date this feature is no longer effective, as a Timestamp |
| Unique_ID | M | AN | Unique ID for each record |
| Country | M | AN | The name of a country represented by its two-letter ISO 3166-1 English country alpha-2 code elements in capital ASCII letters. |
| State | M | A | The name of a state, province or equivalent, as specified in CLDXF or its Canadian equivalent. Example: TX (A1 in RFC 5139) [76] |
| County | C | A | The name of county or county-equivalent as specified in CLDXF or its Canadian equivalent [1]. (A2 in RFC 5139) [76] |
| AdditionalCode | C | A | A code that specifies the geographic area. Used in Canada to hold a Standard |

| ATTRIBUTE NAME | USE M/C | TYPE | DATA DESCRIPTION |
|---|---|---|---|
| | | | Geographical Classification code, which differentiates two municipalities with the same name in a province that does not have counties. |
| Incorporated Municipality | C | A | The name of the incorporated municipality or other general-purpose local governmental unit as specified in CLDXF or its Canadian equivalent. Specify "unincorporated" or "unknown" if necessary. (A3 in RFC 5139) [76] |
| Unincorporated Community | C | A | The name of an unincorporated community, as specified in CLDXF or its Canadian equivalent (A4 in RFC 5139) [76]. |
| Neighborhood Community | C | A | Neighborhood or other informal designation for a part of a community as specified in CLDXF or its Canadian equivalent (A5 in RFC 5139) [76]. |
| AgencyId | M | AN | Unique domain name for the Service. |
| ServiceResponse | M | S | Service supplied for this boundary. May occur more than once. |

### B.8.1 Service Response

| ATTRIBUTE NAME | USE M/C | TYPE | DATA DESCRIPTION |
|---|---|---|---|
| Service URI | M | URI | URI for Routing ex. sip:sos@psap.columbus.oh.us |
| Service URN | M | URN | 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. [58] |
| Service Number | C | AN | The emergency services number appropriate for the location provided in the query. |
| Agency vCard URI | M | URI | URI for the vCARD of contact information. |
| Display Name | C | A | Display Name of the Service ex. Houston FD |

# 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 where such capabilities are desired or required. This appendix assumes that PSAPs and originating networks know when they are operating in an environment where 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, Enhanced Called Party Hold (ECPH), Switch-hook Status, and on/off-hook Ringback.

## 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 IP originating network 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 described in subsequent sections of this Appendix.

### C.1.1 Assumed Behavior in an 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 origination 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) [173] and ATIS-1000666.1999 (2014) [126]. If connection hold is desired/required for the call, the originating network expects to receive a SAP parameter with a 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 an SS7 FAC message that contains 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 downstream from the originating network.

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 off-hook). In this scenario, the originating network is expected to supply audible ringing back towards the PSAP and no 180 Ringing Message should be generated by the Legacy Network Gateway.

### C.1.1.2 MF Signaling from Originating End Office

If Called Party Hold/Switch-hook Status is supported in a legacy origination 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. When the originating end office receives a wink back from the Legacy Network Gateway, 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 Legacy Network Gateway 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 Legacy Network Gateway), through towards the caller. 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 Legacy Network Gateway through to the caller. If the on-hook Ringback feature is invoked by the PSAP attendant on a held connection to a Legacy Network Gateway 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 C3.4.2, the PIF component of the Legacy Network Gateway 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 from the NIF component. Note that neither the originating network nor the Legacy Network Gateway will provide audible ringing toward the PSAP in this case.

### C.1.2 Assumed Behavior in an IP Originating Network

If an IP originating network is operating in a jurisdiction where Called Party Hold/Switch-hook Status is supported, this Appendix assumes that the IP-based originating network will behave in one of the following ways:

1. The originating network follows the procedures defined in PKT-SP-RSTF-109-120412 [174] and PKT-SP-CMSS1.5-I07-120412 [175]. According to Section 8.5.5.8 of PKT-SP-RSTF-109-120412 [174], 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 set to “emergency”, 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 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 that upon receiving a disconnect request from the caller before the PSAP has answered the call, the originating network will send a SIP re-INVITE with an associated SDP set to “inactive” and a Priority header set to “emergency”, and set an ECPH 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 and stop the ECPH 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.

   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. Similarly, if the ECPH timer expires before the call is answered by the PSAP attendant, the originating network is expected to generate a SIP BYE message.

   If the originating network receives a re-INVITE message that contains an Alert-Info header (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) 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. Note that the originating network should not provide audible ring to the PSAP.

2. 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 [59] for handling emergency call originations.

Note: The text above will need to support an SDP offer with an "a=suspended" attribute as described in section C.2.1.1.2, which will be covered in a future revision of this document.

## C.2 Called Party Hold/Switch-hook Status

## C.2.1 Procedures at the Legacy Network Gateway

### C.2.1.1 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 Legacy Network Gateway may contain a Feature Code Indicator in the Service Activation Parameter (SAP) set to "hold available".

#### C.2.1.1.1 Procedures at the PIF Component

Upon receiving an IAM with a SAP, the PIF component of the Legacy Network Gateway will follow the procedures in Section 7.1.1.2.2 and 7.1.1.5, 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-1000679.2013 [167].

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 [186] message, as described in Section 5.4.3 of ATIS-1000679.2013 [167] and send it to the NIF component. This may occur if an emergency call

has been established, Called Party Hold is 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 will contain a Feature Code Indicator in the SAP set to "disconnect request". If the emergency caller subsequently goes "off-hook", the PIF component will receive a 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 7.1.1.5. 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 7.1.1.2.2.

#### C.2.1.1.2 Procedures at the 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 7.1.2.1, 7.1.2.2, and 7.1.2.3 with the following modifications. If, based on provisioning, the NIF component determines that the destination to which the call was delivered (as determined based on the Contact header of the received 180 Ringing or 183 Session Progress message) 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 provisioning, the NIF component determines that the destination to which the call was delivered supports PSAP Call Control Features and the NIF component receives an 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 7.1.1.5 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-1000679.2013 [167] for send a 180 Ringing or 183 Session Progress message to the PIF component.

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 SDP with an "a= suspended" attribute[74]. The re-INVITE message will reference the existing

[74] 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 [176]. The use of

dialog so that the i3 PSAP (or Legacy PSAP Gateway, 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 will include the following information:

- A Request-URI that contains the information provided in the Contact header of the 200 OK message that was returned in response to the original INVITE message;
- A To header that contains the same information as the original INVITE message (i.e., the digits "911");
- A "From" header that contains the same information as in the original INVITE message;
- A Via header that is populated with the element identifier (see Section 3.1.3) for the Legacy Network Gateway;
- A Route header that contains the same information as in the original INVITE (i.e., the ESRP URI obtained from the ECRF);
- A Contact header that contains the same information as in the original INVITE message (i.e., a SIP URI associated with the Legacy Network Gateway);
- 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/Legacy PSAP Gateway (via the NGCS), indicating that it accepts the change, the NIF component will respond to the 200 OK by returning an ACK message toward the i3 PSAP/Legacy PSAP Gateway. The NIF component will 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.

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 will contain the same information described above, except that the SDP will contain the new offer.

Upon receiving a 200 OK message from the i3 PSAP/Legacy PSAP Gateway indicating that it accepts the change, the NIF component will respond to the 200 OK by returning an ACK message toward the i3 PSAP/Legacy PSAP Gateway to acknowledge receipt of the SIP 200 response and to confirm the SDP has been reactivated.

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.

### C.2.1.2 MF Signaling from Originating End Office

#### C.2.1.2.1 Procedures at the PIF Component

Upon receiving a trunk seizure (off-hook) from the originating end office, the PIF component of the Legacy Network Gateway shall return a wink back to the end office. After receiving the called number sequence (i.e., KP + 911 + ST), the PIF component will 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 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 the legacy 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".

The PIF component shall follow the procedures in Section 7.1.1.5 for generating a SIP INVITE message and sending it to the NIF component of the Legacy Network Gateway.

Also, as described in Section 7.1.1.5, the PIF component of the Legacy Network Gateway 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 Legacy Network Gateway 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 will apply audible ringing tone to the calling party.

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. 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 PIF component will 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 [177] (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 [177] (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, as described in Section 7.1.1.1.

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 7.1.1.5, and generate an on-hook signal toward the originating switch.

#### C.2.1.2.2 Procedures at the NIF Component

Upon receipt of an INVITE message from the PIF component, the NIF component shall follow the procedures in Sections 7.1.2.1, 7.1.2.2, and 7.1.2.3 for processing the INVITE message and sending an INVITE to the NGCS. Based on provisioning associated with the incoming trunk group parameters in the Contact header 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 7.1.2.3, 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 (as determined based on the Contact header of the received 180 Ringing or 183 Session Progress message) supports PSAP Call Control Features.

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 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 [177] 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.2.1.1.2, and forward the re-INVITE to the NGCS.

Upon receiving a 200 OK message from the i3 PSAP/Legacy PSAP Gateway (via the NGCS), indicating that it accepts the change, the NIF component will respond to the 200 OK by returning an ACK message toward the i3 PSAP/Legacy PSAP Gateway.

If the NIF component receives an on-hook/"unseize circuit" event indication (encoded using RFC 5244 [177] 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, subsequent to receiving an on-hook/"unseize circuit" event indication, the NIF component receives an off-hook/"seize" event indication (encoded using RFC 5244 [177] 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.2.1.1.2, the re-INVITE will contain the same information as the previous re-INVITE, except that the SDP will contain the new offer.

Upon receiving a 200 OK message from the i3 PSAP/Legacy PSAP Gateway indicating that it accepts the change, the NIF component will respond to the 200 OK by returning an ACK message toward the i3 PSAP/Legacy PSAP Gateway to acknowledge receipt of the SIP 200 OK response and to confirm the RTP has been reactivated.

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 7.1.2.3. 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 7.1.2.3.

### C.2.2 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 will follow normal procedures, as described in RFC 3261 [12], for passing SIP re-INVITE messages and associated responses (200 OK and ACK) associated with requests for Called Party Hold where the originating network and the PSAP support feature-specific signaling.

The ESRP will also follow normal procedures, as described in RFC 3261 [12], for passing SIP BYE messages.

### C.2.3 Procedures at the i3 PSAP

If an i3 PSAP is operating in a jurisdiction where PSAP Call Control features are supported/required, it is expected that 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 of "emergency" and an SDP with attribute "a= inactive" as being associated with PSAP Call Control Features[75]. The i3 PSAP shall use an appropriate mechanism for notifying the PSAP attendant of the change in status[76] (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.3.1.

If an i3 PSAP is operating in a jurisdiction where 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[12] for processing the BYE message, and will

[75] 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-109-120412 [174] and PKT-SP-CMSS1.5-I07-120412 [175] 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" by SBC functionality within the ingress BCF.

[76] 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.



One Nation 9-1-1 One Number

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 [178] for marking the callback call by including a SIP Priority header value of "psap-callback" in the INVITE message associated with the callback call.

## C.2.4 Procedures at the Legacy PSAP Gateway

If the Legacy PSAP Gateway is operating in an environment where PSAP Call Control Features are supported, it will have to support the additional protocol and procedures described below.

### C.2.4.1 Procedures at the NIF Component

The NIF component of the Legacy PSAP Gateway shall follow the procedures described in Section 7.2.2, with the following clarifications. If the NIF component of a Legacy PSAP Gateway receives a re-INVITE message from an NGCS, it will forward that re-INVITE to the PIF component, including an element identifier associated with the Legacy PSAP Gateway in a Via header (see Section 3.1.3).

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.2.1.1.2. Upon receiving an ACK from the NGCS, the NIF component shall forward the ACK to the PIF component.

If a NIF component receives a BYE message from an NGCS, it shall follow the procedures specified in RFC 3261[12] 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 will determine, based on provisioning, whether the PSAP supports PSAP Call Control Features. If the PSAP supports PSAP Call Control Features, the NIF component will generate the re-INVITE message containing an SDP with attribute "a = suspended" described above and send it to the PIF 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 will permit them 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 will 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[12] procedures for processing the BYE and shall send a BYE to the NGCS.

### C.2.4.2 Procedures at the PIF Component

In addition to the procedures specified in Section 7.2.1, the PIF component of the Legacy PSAP Gateway 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.2.4.1.

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 and an SDP with attribute "a=

inactive", the PIF component of the Legacy PSAP Gateway shall apply 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"), it shall stop applying the "on-hook" status alerting, and 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 7.2.4.2.1 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[12] procedures for processing the BYE message and send an on-hook signal to the PSAP.

## C.3 Ringback

The Ringback feature enables the PSAP attendant to invite back an emergency caller, or someone in his surrounding area, into the conversation. 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, 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.3.1 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 phone. 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 Legacy PSAP Gateway.

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[77] 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.

[77] Some deployments may use the P-DCS-OSPS header with a value of "RING" as defined in RFC 5503 to signal Ringback. The specific method being used in one jurisdiction is determined through bilateral negotiations.



One Nation 9-1-1 One Number

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 must initiate a callback to that emergency caller. The callback initiated by the i3 PSAP shall follow the procedures specified in RFC 7090 [178] for marking the callback call by including a SIP Priority header value of "psap-callback" in the INVITE message associated with the callback call.

## C.3.2 Procedures at the Legacy PSAP Gateway

### C.3.2.1 Procedures at the 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 Legacy PSAP Gateway will follow the procedures defined in RFC 4733 [179] for passing DTMF signals to the NIF component of the Legacy PSAP Gateway.

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.3.2.2) in response, it will apply audible ringing on the existing media path to the PSAP.

### C.3.2.2 Procedures at the NIF Component

Upon receiving DTMF information from the PIF component (using RFC 4733 [179] 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 will generate a re-INVITE message toward the emergency caller. The re-INVITE message will contain an Alert-Info header 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 an SDP attribute "a= inactive" with "Priority = emergency"), the ringing tone URI included in the Alert-Info header will typically 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"), the ringing tone URI in the Alert-Info header will be associated with a receiver off-hook/howler tone.

If the Alert-Info header 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 will 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 Legacy PSAP Gateway 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 will

initiate a callback request to/towards that caller. The callback initiated by the NIF component of the Legacy PSAP Gateway shall follow the procedures specified in RFC 7090 [178] for marking the callback call by including a SIP Priority header value of "psap-callback" in the INVITE message associated with the callback call.

### C.3.3 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 will follow normal procedures, as described in RFC 3261 [12], for passing SIP re-INVITE messages and associated responses (200 OK and ACK).

### C.3.4 Procedures at the Legacy Network Gateway

#### C.3.4.1 Procedures at the NIF Component

The NIF component of the Legacy Network Gateway shall be capable of receiving and processing a re-INVITE message that contains an Alert-Info header. If the NIF component receives a re-INVITE message containing an Alert-Info header 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 a SAP that contains 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 [180] for details regarding the coding of the SS7 FAC message).

If the NIF component receives a re-INVITE message containing an Alert-Info header 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.3.4.2 Procedures at the PIF Component

As described in Section C.2.1.1.1, the PIF component of the Legacy Network Gateway 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.

If the PIF component receives a re-INVITE message containing an Alert-Info header, the PIF component shall apply alerting toward the caller appropriate for the audible ringing tone URI provided in the Alert-Info header, and shall return a SIP 180 RINGING message to the NIF component.

.

## C.4 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 resume.

If the originating network supports Enhanced Called Party Hold and the originating switch interconnects with the Legacy Network Gateway via SS7 trunk groups, the ECPH timer must be supported at the Legacy Network Gateway and the external signaling generated by the origination network will be the same as for Called Party Hold. The Legacy Network Gateway will follow the procedures described in Section C.4.1. The Called Party Hold procedures applicable to the ESRP, Legacy PSAP Gateway and PSAP, as described in Section C.2 and its subsections, also apply for Enhanced Called Party Hold when the originating switch interconnects with the Legacy Network Gateway via SS7-controlled trunks.

If the originating network supports Enhanced Called Party Hold and the originating switch interconnects with the Legacy Network Gateway via MF trunk groups, the ECPH timer must be supported at the Legacy Network Gateway and the Legacy Network Gateway will follow the procedures described in Section C.4.2. The procedures at the ESRP, Legacy PSAP Gateway and 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 will be sent by the originating network. The CANCEL message will be processed as specified in RFC 3261 [12] by all elements in the call path. As described in Section 5.2.1.9, if a call arrives at the ESRP but a CANCEL is received prior to any response message being received from an i3 PSAP (or Legacy PSAP Gateway), such that the ESRP is unsure as to whether or not the INVITE message was ever received by the PSAP, the ESRP should notify the PSAP (or Legacy PSAP Gateway) using the AbandonedCall event.

## C.4.1 Procedures at the Legacy Network Gateway for Calls Received over SS7-Supported Trunk Groups

### C.4.1.1 Procedures at the PIF Component

When an originating switch supports Enhanced Called Party Hold and interconnects with the Legacy Network Gateway using SS7-supported trunks, the PIF component of the Legacy Network Gateway will follow the procedures specified in Section C.2.1.1.1.

### C.4.1.2 Procedures at the NIF Component

When an originating switch supports Enhanced Called Party Hold and interconnects with the Legacy Network Gateway using SS7-controlled trunks, the NIF component of the Legacy Network Gateway will follow the procedures specified in Section C.2.1.1.2, with the following clarifications.

If the NIF 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” prior to receiving a 200 OK associated with the emergency call, the NIF component shall perform the following actions. 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 will 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 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.2.1.1.2. Regular Called Party Hold procedures will 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 will send a CANCEL message to the PIF component, as well as to the NGCS.

If, upon receiving the SIP INFO message with the SAP set to "disconnect request" from the PIF component, the NIF component determines that Enhanced Called Party Hold is not supported for the incoming trunk group, it will not set the ECPH timer and will send a CANCEL message to the PIF component as well as to the NGCS.

## C.4.2 Procedures at the Legacy Network Gateway for Calls Received over MF Trunk Groups

### C.4.2.1 Procedures at the PIF Component

When an originating switch supports Enhanced Called Party Hold and interconnects with the Legacy Network Gateway using MF trunks, the PIF component of the Legacy Network Gateway will follow the procedures specified in Section C.2.1.2.1, 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 will 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 [177] (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 [177] (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.

### C.4.2.2 Procedures at the NIF Component

When an originating switch supports Enhanced Called Party Hold and interconnects with the Legacy Network Gateway using MF trunks, the NIF component of the Legacy Network Gateway will follow the procedures specified in Section C.2.1.2.2, with the following exceptions.

If the NIF receives an on-hook/"unseize circuit" event indication from the PIF component (encoded using RFC 5244 mechanisms or equivalent) prior to receiving a 200 OK associated with the emergency call, 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 will initiate an ECPH timer which indicates the maximum length of time that Enhanced Called Party Hold will be active. As described in Section C.4.1.2, the timer should be provisionable.

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.2.1.2.2. Regular Called Party Hold procedures will 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 will send a CANCEL message to the PIF component, as well as to the NGCS.

If, upon receiving the on-hook/"unseize circuit" indication from the PIF component, the NIF component determines that Enhanced Called Party Hold is not supported for the incoming trunk group, it will not set the ECPH timer and will send a CANCEL message to the PIF component as well as to the NGCS.



One Nation 9-1-1 One Number

# Appendix D – Example Call Flows (informative)

This section provides example end-to-end i3 call flows. The first example described a call flow where all data is provided by value. An example call flow where data is provided by reference will be added in a future revision 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:

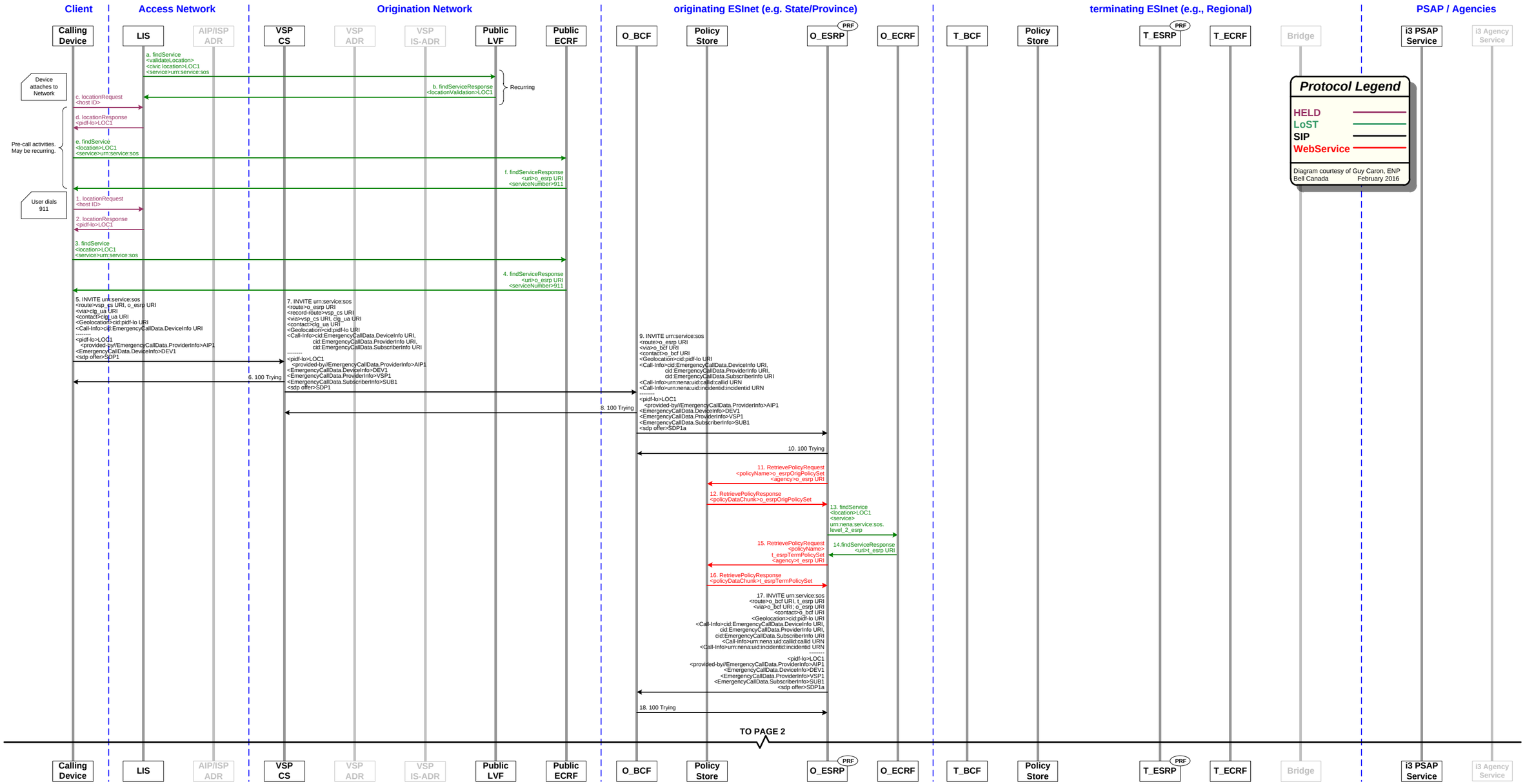
- SIP end-to-end call;
- AIP and VSP are not vertically integrated;
- AIP and ISP are vertically integrated;
- The Calling Device is nomadic;
- The Calling Device is identifiable and authenticable by the LIS to reside within its administrative domain;
- The location format is Civic;
- The provisioned 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 pointing to the VSP CS in dialog-initiating requests[78]);
- 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 LCP
- The Policy Store is external to the ESRP but within its ESInet;
- ESRPs have already collected the Origination and Termination Policy names at call time (enumeratePolicyRequest/enumeratePolicyResponse flows not shown);
- BCFs outside ESInets are not shown;
- All SIP Proxies are Transaction stateful;
- Egress BCFs do not anchor media;
- 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 pointing to the BCF in dialog-initiating requests);

[78] Most devices don't include a Route header 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 RFC3261.

- 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.

•

• **Figure D1. Diagram Example i3 Call Flow – Data Provided by Value – Part 1**

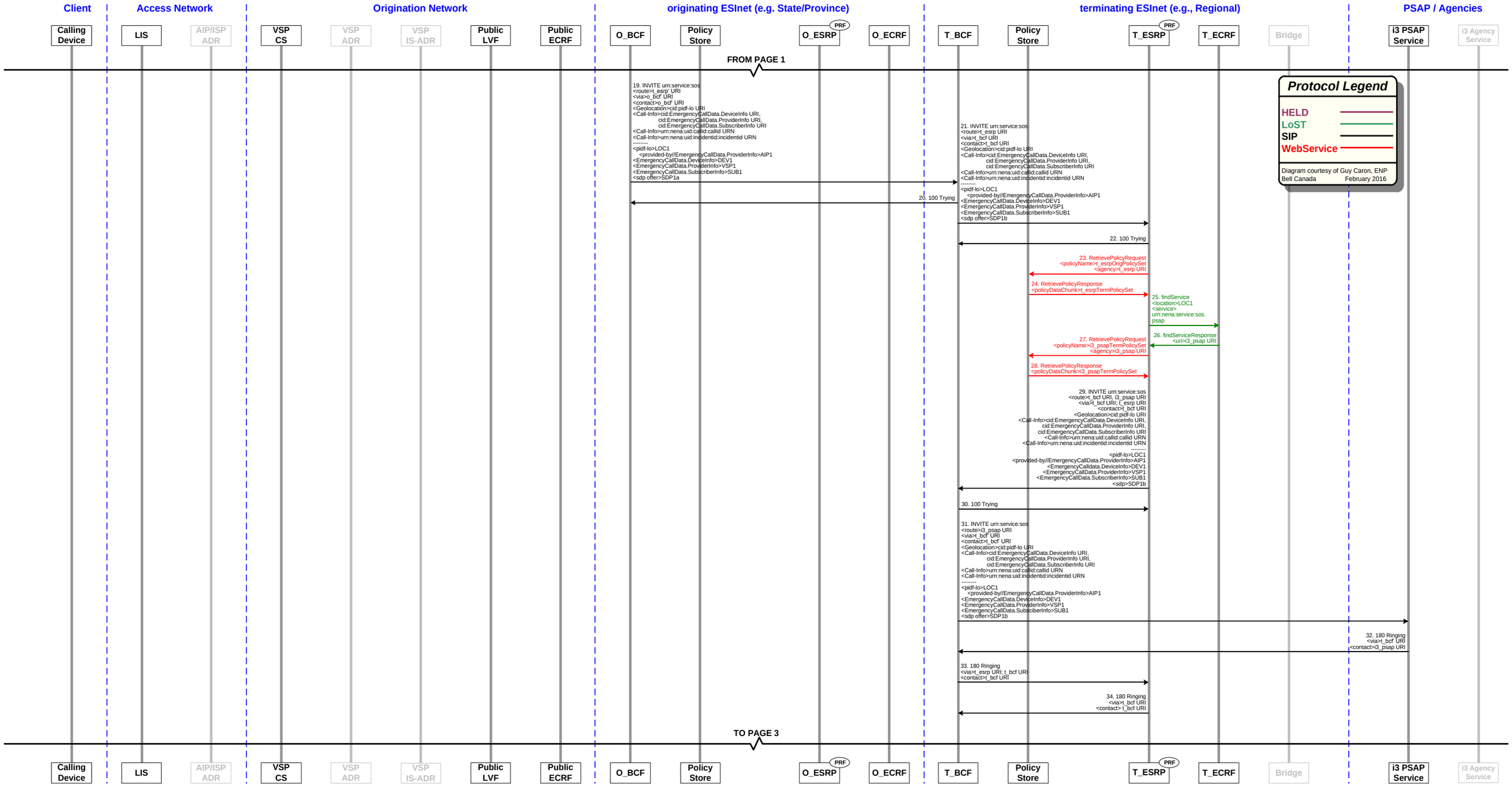





One Nation 9-1-1 One Number

•

• **Figure D1. Diagram Example i3 Call Flow – Data Provided by Value – Part 2**

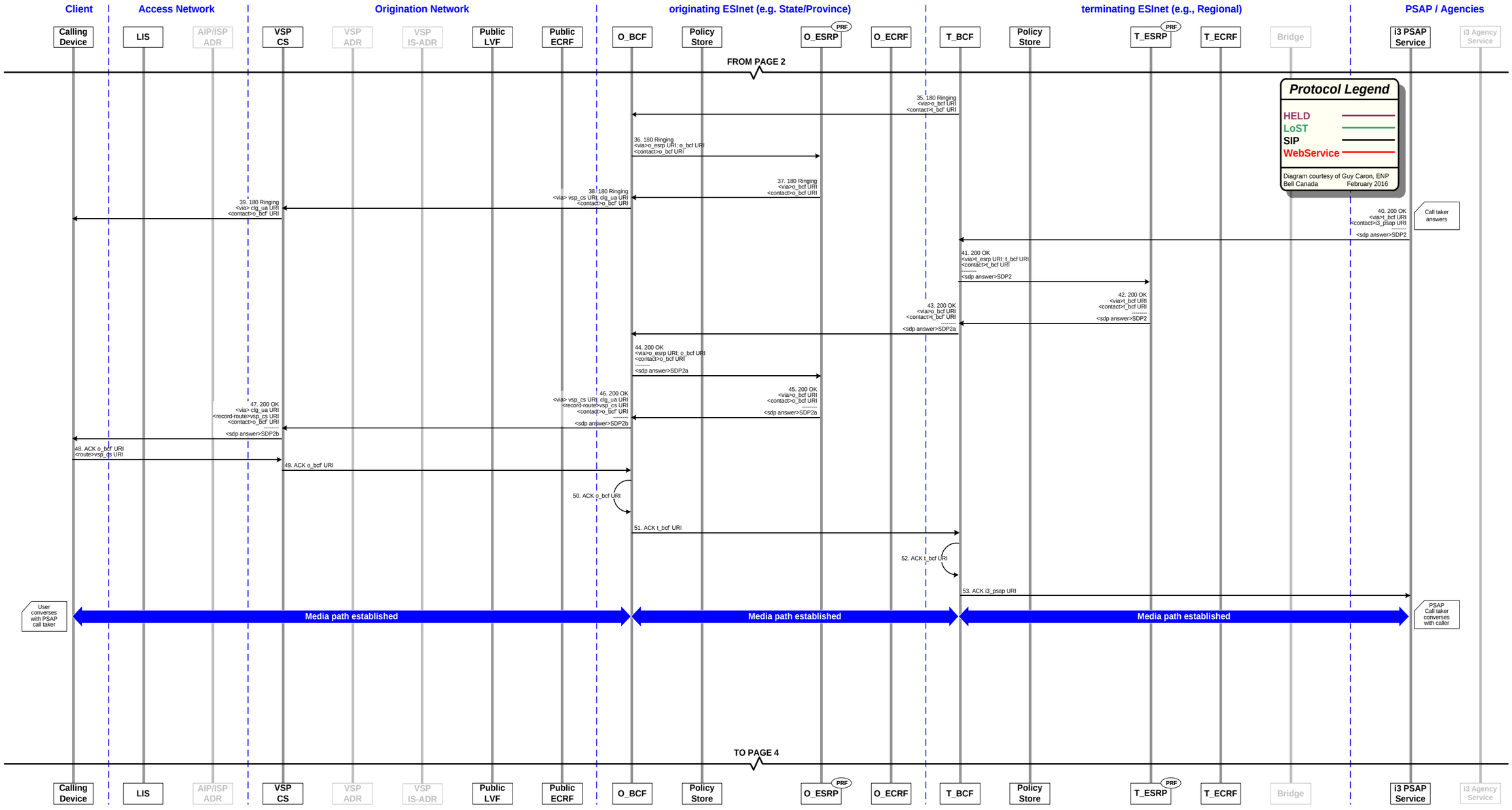





One Nation 9-1-1 One Number

•

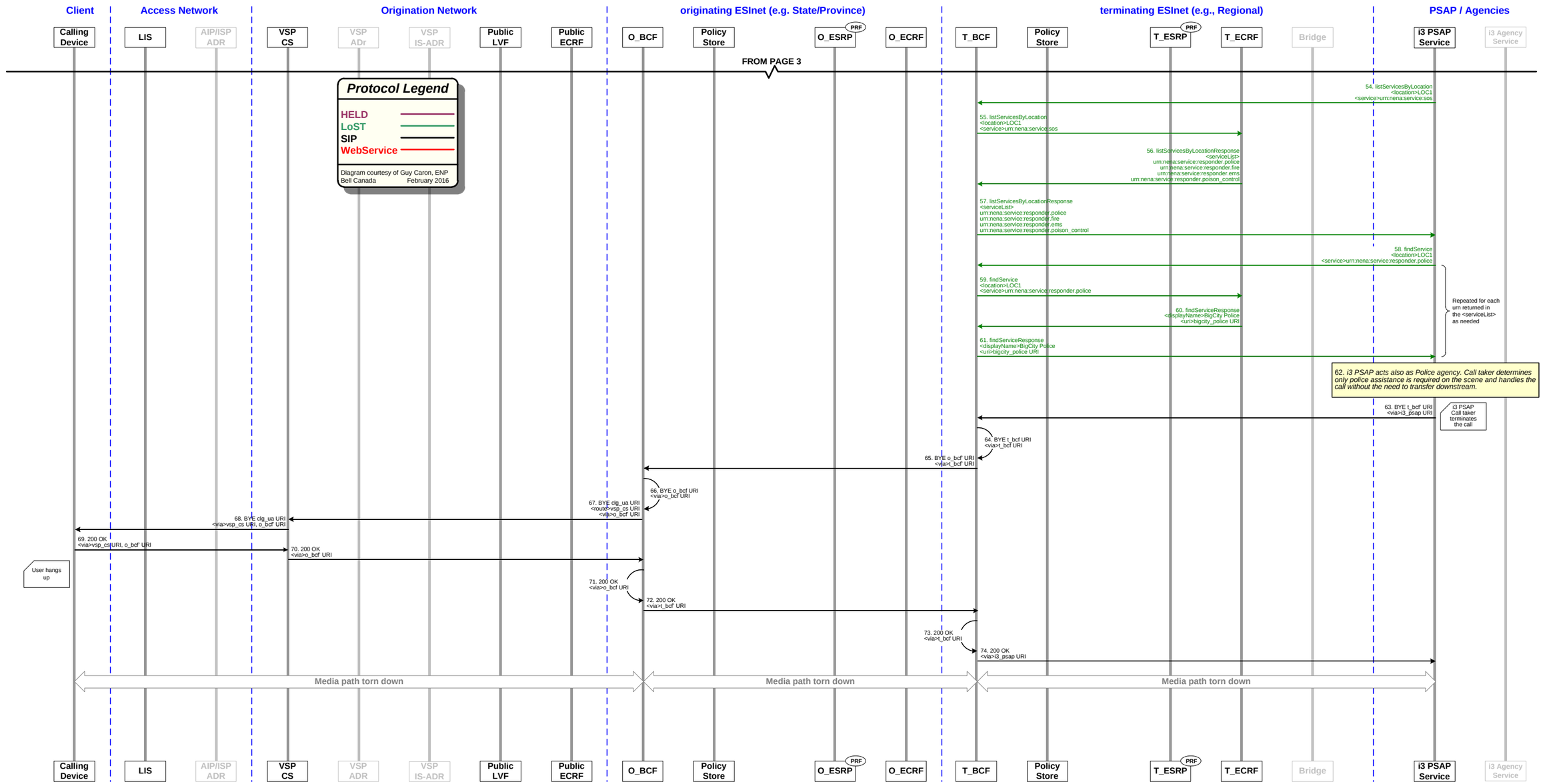
• **Figure D1. Diagram Example i3 Call Flow – Data Provided by Value – Part 3**






One Nation 9-1-1 One Number

- **Figure D1. Diagram Example i3 Call Flow – Data Provided by Value – Part 4**






One Nation 9-1-1 One Number

## D.2 Step-by-step description

### D.2.1 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.2.2 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 an HELD locationResponse containing a PIDF-LO representation of civic address "LOC1", including the element <provided-by> populated with the access provider ID "AIP1".

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 it is attached to. 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 goes for the LoST findService request.*

### D.2.3 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 dialstring "911" as the emergency service number in the area of location "LOC1" (by comparing it to what was previously discovered in step e), enters in an "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 an 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.
5. The Calling SIP UA sends an INVITE with the Request URI set to "urn:service.sos", a Route header set to the VSP CS (outbound proxy), another Route header set to the value received in the LoST response of step 2 ("o_esrp URI"), a Contact header for itself ("clg_ua URI") and a Geolocation header 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 referring to itself and adds Via and Record-Route headers pointing to itself ("vsp_cs URI"). It also adds Call-Info header fields, 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 ("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, authenticates the VSP CS (steps not shown) and replies with a provisional 100 Trying SIP response to the VSP CS.
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 set to "o_esrp URI", Via and Contact headers pointing to itself ("o_bcf URI") and an SDP offer "SDP1a". It generates Call and Incident tracking identifiers and adds Call-Info header fields containing them with purpose parameters of "nena-CallId" and "nena-IncidentId" respectively. It also copies the other elements found in the body of the incoming INVITE. The O_BCF then performs a DNS lookup on the URI found in the Route header ("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 referring to it.
11. The O_ESRP is statically provisioned with the address of its Policy Store. It formulates a webService call (RetrievePolicyRequest with <policyName> as "o_esrpOrigPolicySet" and <agency> as the agency ID of the agency responsible for O_ESRP, "o_esrp URI") to retrieve the originating policies associated with it. Credentials are also provided.
12. The Policy Store is provisioned with all the policies associated with its serving clients (step not shown). It receives the RetrievePolicyRequest, authenticates the O_ESRP then dips into its database to find an associated record. It returns the result in a RetrievePolicyRequestResponse with the originating policies for O_ESRP in the <policyDataChunk> ("o_esrpOrigPolicySet").
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 originating policy contains a rule with a LoSTServiceURN condition which 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 parameter: <location> "LOC1" as found in the body of the INVITE, <service> "urn:nena: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:nena: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 and determines it requires the associated termination policies associated with "t_esrp URI". As such, it formulates a webService call (RetrievePolicyRequest with policy name as "t_esrpTermPolicySet" as the agency ID of the agency responsible for T_ESRP, "t_esrp URI") to retrieve the terminating policies associated with T_ESRP. Credentials are also provided.

16. The Policy Store receives the RetrievePolicyRequest, authenticates the O_ESRP then dips into its database to find an associated record. It returns the result in a RetrievePolicyRequestResponse with the terminating policies for T_ESRP in the <policyDataChunk> ("t_esrpTermPolicySet").
17. The O_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 T_ESRP. The O_ESRP adds a Route header set to "t_esrp URI" and adds a Via header pointing to itself ("o_esrp URI"). Following its provisioned behavior for all calls exiting the local ESInet, the O_ESRP then adds a top Route header populated with its desired next hop "o_bcf URI", 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.
19. The O_BCF behaves as a full B2BUA[79] and terminates the ingress dialog. On the egress side, it creates a new dialog by sending an INVITE populated with a Route header set to "t_esrp' URI", a Via header pointing to itself ("o_bcf' URI") and copies the Call-Info 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 ("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[71], 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 set to "t_esrp URI", Via and Contact headers pointing to itself ("t_bcf URI") and an SDP offer "SDP1b". It also copies the Call-Info 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 ("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 referring to it.

[79] Topology hiding may occur between ESInets, but consideration should be given to not doing so in support of improved ability to diagnose problems.

23. The T_ESRP is statically provisioned with the address of its Policy Store. It formulates a webService call (RetrievePolicyRequest with <policyName> as "t_esrpOrigPolicySet" and <agency> as the agency ID of the agency responsible for T_ESRP, "t_esrp URI") to retrieve the originating policies associated with itself. Credentials are also provided.
24. The Policy Store is provisioned with all the policies associated with its serving clients (step not shown). It receives the RetrievePolicyRequest, authenticates the T_ESRP then queries its database to find an associated record. It returns the result in a RetrievePolicyRequestResponse with the originating policies for T_ESRP in the <policyDataChunk> ("t_esrpTermPolicySet").
25. The T_ESRP invokes its internal PRF that processes the rules in the policy received and applies them to the incoming INVITE (step not shown). The originating policy contains a rule with a LoSTServiceURN condition that 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 parameter: <location> "LOC1" as found in the body of the INVITE, <service> "urn:nena: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:nena:service:sos.psap", and returns a LoST findService Response with the URI of the next hop ("i3_psap URI") to the T_ESRP.
27. The T_ESRP receives the LoST response and determines it requires the associated termination policies associated with "i3_psap URI". As such, it formulates a webService call (RetrievePolicyRequest with policy name as "i3_psapTermPolicySet" as the agency ID of the agency responsible for i3_PSAP, "i3_psap URI") to retrieve the terminating policies associated with i3_PSAP. Credentials are also provided.
28. The Policy Store receives the RetrievePolicyRequest, authenticates the T_ESRP then queries its database to find an associated record. It returns the result in a RetreivePolicyRequestResponse with the terminating policies for i3_PSAP in the <policyDataChunk> ("i3_psapTermPolicySet").
29. 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 set to "i3_psap URI" and adds a Via header pointing to itself ("t_esrp URI"). Following its provisioned behavior for all calls exiting the local ESInet, the T_ESRP then adds a top Route header populated with its desired next hop "t_bcf URI", 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[71] and terminates the ingress dialog. On the egress side, it creates a new dialog by sending an INVITE populated with a Route header set to "i3_psap URI", a Via header pointing to itself ("t_bcf" URI") and copies the Call-Info 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 ("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[80] SIP response to the URI found in the top Via header ("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 headers of the associated ingress INVITE pointing to the T_ESRP.
34. The T_ESRP receives the provisional 180 Ringing message, removes the Via header referring to it and forwards the response to the next URI in the Via header, 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 headers 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 headers of the associated ingress INVITE pointing to the O_ESRP.
37. The O_ESRP receives the provisional 180 Ringing message, removes the Via header referring to it and forwards the response to the next URI in the Via header, 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 headers of the associated ingress INVITE pointing to the VSP CS. It provides a different value in the Contact header ("o_bcf' URI").
39. The VSP CS receives the provisional 180 Ringing message, removes the Via header referring to it and forwards the response to the next URI in the Via header, 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 applies a ringing 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 ("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 headers of the associated ingress INVITE pointing to the T_ESRP.

[80] The 180 Ringing message may be preceded by a 100 Trying message.

42. The T_ESRP receives the final 200 OK message, removes the Via header referring to it and forwards the response to the next URI in the Via header, 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 headers 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 ("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 headers of the associated ingress INVITE pointing to the O_ESRP.
45. The O_ESRP receives the final 200 OK message, removes the Via header referring to it and forwards the response to the next URI in the Via header, 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 headers of the associated ingress INVITE pointing to the VSP CS. Because it anchors media on ingress, the SDP answer is now "SDP2b". It also provides a different value in the Contact header ("o_bcf' URI").
47. The VSP CS receives the final 200 OK message, removes the Via header referring to it and forwards the response to the next URI in the Via header, 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 headers set to the values of its route-set. It sets the RequestURI to the value of the Contact header ("o_bcf' URI") and sends the ACK to the top Route header, in this case, the VSP CS.
49. The VSP CS removes the Route header referring to it and forwards the ACK using the RequestURI ("o_bcf' URI").
50. The O_BCF behaves as a full B2BUA[71]. On the egress side, it sends an ACK populated with a RequestURI set to "o_bcf URI" found in the Contact header of the associated 200 OK response (step 44).
51. The O_BCF behaves as a full B2BUA[71] and terminates the ingress dialog. On the egress side, it uses the previously opened egress dialog and sends an ACK populated with a RequestURI set to "t_bcf' URI" found in the Contact header of the associated 200 OK response (step 43).
52. The T_BCF behaves as a full B2BUA[71] and terminates the ingress dialog. On the egress side, it uses the previously opened egress dialog and sends an ACK populated with a RequestURI set to "t_bcf URI" found in the Contact header of the associated 200 OK response (step 41).
53. 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 RequestURI set to "i3_psap URI" found in the Contact header 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 through 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:nena: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 let 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:nena:service:responder.police", "urn:nena:service:responder.fire", "urn:nena:service:responder.ems" and "urn:nena: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 let the message go through to the i3 PSAP.
58. With the list of available services in hand, the i3 PSAP proactively launches LoST findService requests 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:nena: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 let 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:nena: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 let 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 headers previously populated for its dialog(s) to populate the Route headers and RequestURIs. 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.

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.*