EENA NG112 Document

Next Generation 112
Long Term Definition

Title:	Long Term Definition
Version:	1.1
Code:	LTD_v1.1.doc
Revision Date:	03-06-2013

Contributors

The National Emergency Number Association (NENA) VoIP/Packet Technical Committee Long Term Definition Working Group developed the "Detailed Functional and Interface Specification for the NENA i3 Solution – Stage 3" standard.

The Next Generation 112 Long Term Definition document is based on the NENA i3 Stage 3 technical specification. EENA therefore recognizes the work done by the members of NENA.

The following members of the Next Generation 112 Technical Committee have contributed to this release of the document:

Name	**Company**
Andrei Grososiu	Special Telecommunications Service – RO
Cristina Lumbreras	EENA
Hannes Tschofenig	Nokia Siemens Networks / EENA
Helmut Wittmann	Siemens Enterprise Communications
Gunnar Hellström	Omnitor
John Medland	BT
Brian Rosen	Neustar
Emmanuel Buu	IVES
Laurent Faucillon	France Telecom/Orange
Randall Gellens	Qualcomm
Massimo Cristaldi	IES Solutions
Ian Colville	ACULAB
Andrew Hutton	Siemens Enterprise Communications

TABLE OF CONTENTS

1 Introduction

1.1 Overview

It is estimated that 320 million emergency calls are made every year in the European Union, enabling emergency services to assist citizens in all sorts of difficult situations. For the time being however, most European emergency services can only be reached through the public switched telephony or mobile networks.

Voice over Internet Protocol (VoIP) based devices and applications have become commonplace. Citizens use them to conveniently communicate, send and receive information. Text messaging is an ever more common communication means, replacing the traditional two-way voice telephone call. Pictures and videos from phones and PDAs are shared instantly with friends and colleagues around the world, and social networks have become a media by themselves. Video and text based communications are replacing traditional systems such as teletypes for the deaf and hard of hearing. Cars are being fitted with telematics systems that automatically initiate a voice call and provide valuable data when a car is involved in an accident (eCall). Geographical location based services are increasingly used to submit or lookup close points of interest or friend’s current position. Modern mobile phones from which an emergency call might be placed have the potential to transmit life saving location information with the call. Enterprise workers expect to be able to place an emergency call from a campus or remote building complex environment and have a first line response dispatched to the specific location, be that a building within a campus or a floor in a building or an office on a floor.

All over the world, citizens expect to be able to contact emergency services with technologies they use to communicate every day. Thus, European citizens have clear expectations about the availability of 112 emergency services with enhanced capabilities of technologies being used in daily life.

However, the existing, legacy emergency services infrastructure (circuit switched telephony for 112 telephone calls, not data) is not designed in a way that enables interaction with enhanced services, or that current and future communications and operational requirements will be met. Simply put, the emergency services infrastructure has not kept up with technology, thus, is not able to provide the level of service that citizens expect.

Hence, a new technology with a new architecture is needed to resolve these issues – the “Next Generation 112 architecture (NG112)”. NG112 enables citizens to contact emergency services in different ways, using the same types of technology as those they use to communicate every day. It also makes possible that 112 PSAPs receive more and better information about emergencies of all magnitudes and improves interoperability between emergency services. Consequently, response time and operation cost will be reduced, while effective response will increase significantly.

NG112 addresses three major objectives:

1. Communication between citizens and emergency services: NG112 is designed to enable citizens to reach an authority (e.g., PSAP) by calls using VoIP, text messaging, real-time text, pictures and video. It could also provide emergency services with more data, such as location and health data. NG112 enables the delivery of calls, messages and data to the appropriate PSAP and other appropriate emergency entities, and adds significant value to the call handling process.
2. Interoperability between emergency services: NG112 enables several Public Safety Answering Points (PSAPs) to be part of a common emergency services IP network, providing them with redundancy and interoperability features. This network should support data and communications needs for coordinated incident management between PSAPs, and provide a reliable and secure environment for emergency communications.
3. Open Standards approach: NG112 is based on Internet Protocol (IP)-network based standard interfaces between all forms of communications components. For instance ECRIT and Geopriv working groups in the IETF NG112 have already defined standards applicable to Next Generation 112. Hence, existing off-the-shelf hardware and software can be deployed, which increases the technical commonalities between EU member states, drives TCO and fosters the European public safety eco-system. Existing experience from other regions, namely NENA in the US, with its significant work on the NG911 architecture definition and couple with pilot and certification experience, is carefully examined in the NG112 approach and where necessary, adapted to European needs.

Concluding, the evolutionary path towards NG112 lies in opening emergency services access to the Internet. Besides, access to emergency services is a highly sensitive public safety segment. Thus, equally important to enabling technology, is the fact that NG112 also requires the revision of EU and national emergency services policies, regulations and statutes.

As a first step, though, the aim of this document is to describe the underlying technical principles, which are closely aligned with EU public authorities and PSAP requirements [EENA survey 06/11].

As pointed out already, significant work in standards and technologies has been accomplished, already. Therefore, the European Emergency Number Association Next Generation 112 Technical Committee has decided to take the NENA Detailed Functional and Interface Specification for the NENA i3 Solution – Stage 3 [148] as a blue print and adapt it to European standards and emergency services requirements.

The purpose of this work is to define a long-term definition of an European emergency services architecture. The document starts with the definition of specific terminology used in the description of the NG112 architecture. Next sections describe elements building the core concept of the NG112 architecture: the Emergency Services IP Network (ESInet). The ESInet is an emergency services network of networks that utilizes IP technology. ESInets are private, managed, and routed IP networks. An ESInet can serve a set of PSAPs, a region, a state, or a set of states. ESInets may be interconnected and have to be built upon common functions and interfaces making ESInets interoperable. This specification defines a number of Functional Elements (FEs), with their external interfaces. It is also important to mention that NG112 architecture needs to be secure against various attacks.

All PSAPs will have to be able to handle calls originated by different types of networks, such as over-the-top VoIP providers, 3GPP IMS networks [64], enterprise networks, as well as legacy circuit switched networks. This document describes how 112 works after transition. Reality is that not all PSAPs will be compatible with NG112 at the same time. These are the main facts that make gateways a crucial element in the architecture. Legacy-based PSAPs are connected to the ESInet via a gateway (the Legacy PSAP Gateway). The definition of the Legacy PSAP Gateway is broad enough that both primary and secondary PSAPs that have not been upgraded may be served by this type of gateway.

This document describes the “end state” that has been reached after a migration from legacy TDM circuit-switched telephony, and the legacy E112 system built to support it, to an all IP-based telephony 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. A certificate authority that issues certificates to different entities in the emergency services networks has to be created. This enables proper authentication, and builds the foundation for authorization. The overall level of security will be substantially improved as a consequence.
2. All calls entering the ESInet are SIP based. Gateways, if needed, are outside of, or on the edge of, the ESInet. IP services that are not native SIP based, have protocol interworking to SIP prior to being presented to the ESInet.
3. Access Network Providers (e.g., 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 is critical for 112 calls because it provides the ability for PSAP call takers to make decisions based on location and to dispatch first responders without undue delay to the person in need for help.
4. All calls entering the ESInet will normally have location (which might be coarse grained, e.g., cell site/sector) in the signaling with the call. This will allow for location based routing.
5. The Location Validation Function (LVF) and Emergency Call Routing Function (ECRF) are available. The LVF ensures that entered civic location information had been validated prior to its usage and ECRFs allow dynamic call routing based on location, and on additional policy information.

6. 112 authorities have accurate GIS systems, which are used to provision the LVF and ECRF.
7. Civic location will be validated prior being used in an emergency call. This ensures that civic location that is incorrect can be detected early in the process. Periodic revalidation of civic location against the LVF is also needed 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 LTD architecture defines a Legacy Network Gateway (LNG) to interface between the legacy network and the ESInet.
9. PSAPs may not have upgraded and the LTD architecture describes a Legacy PSAP Gateway (LPG) to interface between the ESInet and a legacy PSAP. The LPG supports the origination of an emergency call through the ESInet to a legacy PSAP as well as the transfer of an emergency call from/to an LTD PSAP to/from a legacy PSAP.
10. Applicable laws, regulations and rules may need to be enhanced to support NG112 system deployment.
11. Creation of a Public Safety Computer Emergency Response Team (CERT) is anticipated.

1.2 Operational Impacts Summary

This standard will have a profound impact on the operation of 112 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 112 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.

1.3 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 Internet to accept calls. This means that PSAPs will likely experience deliberate attack on their systems. The types of vulnerabilities that NG112

systems must manage and protect against will fundamentally change and will require constant vigilance to create a secure and reliable operating environment. NG112 systems must have robust detection and mitigation mechanisms to deal with such attacks.

2 Recommendation for Future Work

There are several sections where it is noted that further work is needed, and future editions will cover topics in more depth.

There is, however, work that is currently intentionally out of scope for this specification, namely

- the communication interaction with first reponders using IP/SIP-based communication protocols, and
- configuration and implemenation aspects of the emergency services infrastructure.

The following table lists sections in this document that refer to possible future work.

This document makes use of the System for Cross-domain Identity Management (scim) to provision user accounts. More detailed descriptions are needed
This document still uses vCards instead of the XML-based representation (called xCards).
A list of the parameters contained in the notification of the ESRPnotify Event Package will be provided in a future edition of this document
Specific policy document structures will be specified for each of the policy instances defined for the ESRP in a future edition of this document.
While all NG112 PSAPs must handle all media, a legacy PSAP behind an LPG would only handle voice media and text phones. There is no mechanism by which a caller could discover what media the PSAP supports. This will be covered in a future edition of this document.
Logging: The LNG must log all significant events but various log formats have not been specified yet. For example, it may be desirable to log other messages that are part of the INVITE transaction, such as the ACK. Furthermore, a mechanism to discover the logger associated with an agency will be provided in a future edition of this document.
The description of the Legacy Network Gateway currently puts a strong emphasis on voice. A future version of the document may provide mappings for other media as well. Examples are in-vehicular emergency services support using eCall, or SMS-based emergency services support.

The creation of a certificate authority for usage with emergency services organizations is needed. This will help to ensure proper authentication and authorization of electronic communication within each organization as well as between organizations.
This version of the document does not describe how the IP interconnection agreements are accomplished nor how the SIP-level peering agreements are established. These are assumed to be outside the scope of this document. In the area of SIP interconnection various standards are available. A future version of this document will describe this work.
This document supports non-human initiated calls, for example, using sensors transmitting alerts. For interworking with the emergency services infrastructure a SIP-based mechanism utilizing CAP payloads is described. When sensors use HTTP or CoAP for their communication of sensor readings then a translation gateway to SIP is needed. A future version of this document may define additional protocols for emergency services networks to utilize HTTP or CoAP directly without any need to convert messages to SIP.
This version does not describe interworking between SIP/HELD and E2/MLP/SUPL for location conveyance and location updates. This will be covered in a future edition of this document.
PSAP management interface will be provided in a future edition of this document.
Roles for usage with an access control policy will be added in a future edition of this document.
The European Emergency Services Registry Service (ERS) has to be established.

3 Terminology and Acronyms

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

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-associated 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 NG112. The term "Incident" is used to refer to a real world occurrence for which one or more calls may be received.

The following acronyms are used in this document:

Acronym	***Description***
3GPP	3rd Generation Partner Project
3GPP2	3rd Generation Partnership Project 2
AAA	Authorization, Admission and Accounting
ABNF	Augmented Backus-Naur Form
ACK	Acknowledgement
ACM	Address Complete Message
AES	Advanced Encryption Standard
AIP	Access Infrastructure Provider
AMR	Adaptive Multi Rate (codec)
AMR-WB	Adaptive Multi Rate (codec) – Wide Band
ANI	Automatic Number Identification
ANS	American National Standard
ANSI	American National Standards Institute
AoR	Address of Record
APCO	Association of Public Safety Communications Officials
ATIS	Alliance for Telecommunications Industry Solutions
ATIS-ESIF	Alliance for Telecommunications Industry Solutions – Emergency Services Interconnection Forum
B2BUA	Back to Back User Agent
BCF	Border Control Function
BISACS	Building Information Services and Control System
CA	Certificate Authority
CAD	Computer Aided Dispatch
CAMA	Centralized Automatic Message Accounting
CAP	Common Alerting Protocol

CERT	Community Emergency Response Team
cid	Content Indirection
CIDB	Call Information Database
CPE	Customer Premises Equipment
CRL	Certificate Revocation List
CS	Circuit Switched
CSCF	Call Session Control Function
CSP	Communication Service Provider
DHCP	Dynamic Host Control Protocol (i2) Dynamic Host Configuration Protocol
DNS	Domain Name Server (or Service or System)
DoS	Denial of Service
DSL	Digital Subscriber Line
E112	Enhanced 112
EC	European Commission
ECRF	Emergency Call Routing Function
Ecrit	Emergency Context Resolution In the Internet
E-CSCF	Emergency Call Session Control Function
EDXL	Emergency Data eXchange Language
EENA	European Emergency Number Association
EES	European Emergency Services
EISI	Emergency Information Services Interface
ERS	European Emergency Services Registry Service
ESIF	Emergency Services Interconnection Forum
ESInet	Emergency Services IP Network
ESMI	Emergency Services Messaging Interface
ESNet	Emergency Services Network
ESN	Emergency Service Number, Electronic Serial Number, Emergency Service Network
ESNI	Emergency Services Network Interfaces
ESQK	Emergency Services Query Key

ESRK	Emergency Services Routing Key
ESRP	Emergency Services Routing Proxy
ESZ	Emergency Services Zone (Same as ESN)
EVRC	Enhanced Variable Rate Narrowband Codec
EVRC-WB	Enhanced Variable Rate Wideband Codec
FCC	Federal Communications Commission
GDP	Generic Digit Parameter
Geopriv	Geolocation and Privacy
GeoRSS	Geodetic Really Simple Syndication
Geoshape	Geodetic Shape
GML	Geographic Markup Language
GSM	Global Standard for Mobile Communication
GUID	Globally Unique Identifier
HELD	HTTP-Enabled Location Delivery Protocol
HSS	Home Subscriber Server
IAM	Initial Address Message
IANA	Internet Assigned Numbers Authority
IDP	Identity Provider
IETF	Internet Engineering Task Force
IM	Instant Messaging
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IP-CAN	IP Connectivity Access Network
IP-PBX	Internet Protocol Private Branch Exchange
IPsec	Internet Protocol Security
ISDN	Integrated Services Digital Network
ISUP	Integrated Services Digital Network User Part
ISP	Internet Service Provider
ISUP	Integrated Services Digital Network User Part
KP	Key Pulse

LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LIF	Location Interwork Function
LIS	Location Information Server
LO	Location Object
LoST	Location to Service Translation
LRF	Location Retrieval Function
LTD	Long Term Definition
LVF	Location Validation Function
MDN	Mobile Directory Number
MEP	Message Exchange Pattern
MF	Multi-Frequency
MIB	Management Information Base
MPC/GMLC	Mobile Positioning Center/ Gateway Mobile Location Center
MSC	Mobile Switching Center
MPLS	Multi-Protocol Label Switching
MSAG	Master Street Address Guide
MSC	Mobile Switching Center
MSRP	Message Session Relay Protocol
MTP	Message Transfer Point
NAT	Network Address Translation
NCIC	National Crime Information Center, National Crime Enforcement Center
NENA	National Emergency Number Association
NG112	Next Generation 112
NGES	Next Generation Emergency Services
NGN	Next Generation Network
NIF	NG112 Specific Interwork Function
NMC	112 Malicious Content
NPD	Numbering Plan Digit

NTP	Network Time Protocol
OASIS	Organization for the Advancement of Structured Information Standards
OGC	Open Geospatial Consortium
OLIP	Originating Line Information Parameter
PAI	P-Asserted-Identity
P-CSCF	Proxy Call Session Control Function
PCA	PSAP Credentialing Agency
PDA	Personal Digital Assistant
PHB	Per Hop Behaviors
PIDF	Presence Information Data Format
PIDF-LO	Presence Information Data Format – Location Objects
PIF	Protocol Interworking Function
PKI	Public Key Infrastructure
PRF	Policy Routing Function
PSP	Provisioning Service Provider
PSAP	Public Safety Answering Point or Primary Public Safety Answering Point
PSO	Provisioning Service Object
PSTN	Public Switched Telephone Network
PTSC	Packet Technologies and Services Committee (ATIS Standards Committees)
QoS	Quality of Service
RA	Requesting Authority
RBAC	Role Based Access Control profile
RDF	Routing Determination Function
REL	Release (message)
REST	Representational State Transfer
RFC	Request for Comments
RG	Response Gateway, Routing Gateway
RLC	Release Complete (message)

ROHC	Robust Header Compression
RTCP	Real Time Control Protocol
RTP	Real Time Transport Protocol
RTSP	Real Time Streaming Protocol
RTT	Real Time Text
S-CSCF	Serving Call Session Control Function
SAML	Security Assertion Markup Language
SBC	Session Border Control
SCTP	Session Control Transport Protocol
SDES	Session Description protocol Security Descriptions
SDO	Standards Development Organization
SDP	Session Description Protocol
SHA	Secure Hash Algorithm
SIF	Spatial Information Function
SIO	Service Information Octet
SIP	Session Initiation Protocol
SMS	Short Message Service
SOA	Service Oriented Architecture
SOAP	Simple Object Access Protocol
SPML	Service Provisioning Markup Language
SR	Selective Routing, Selective Router
SRTP	Secure Real Time Protocol
SRV	Service (a DNS record type)
SS7	Signaling System 7
TCP	Transport/Transmission Control Protocol
TDM	Time Division Multiplexing
TLS	Transport Layer Security
TN	Telephone Number
TOPS	Technology and Operations Council
TRD	Technical Requirements Document

text phones	Teletypewriter (a.k.a. TDD, Telecommunications Device for the Deaf and Hard-of-Hearing)
UA	User Agent
UAC	User Agent Client
UAS	User Agent Service
UDDI	Universal Description, Discovery and Integration
UDP	User Datagram Protocol
UE	User Element
URI	Uniform Resource Identifier
URISA	Urban and Regional Information Systems Association
URL	Uniform Resource Locator (location sensitive)
URN	Uniform Resource Name (location insensitive)
USPS	United States Postal Service
UTC	Universal Coordinated Time
VEDS	Vehicle Emergency Data Sets
VF	Validation Function
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
VSP	VoIP Service Provider
WFS	Web Feature Service
WSDL	Web Service Definition Language
WSS	Web Services Security
WTSC	Wireless Technologies and Systems Committee
XACML	eXtensible Access Control Markup Language
XML	eXtensible Markup Language
XMPP	eXtensible Messaging and Presence Protocol
XSD	W3C XML Schema Definition

The following terms are used in this document.

Term	*Definition*
g.711 a-law	An ITU-T Recommendation for an audio codec for telephony in non-North American regions

Term	*Definition*
g.711 mu-law	An ITU-T Recommendation for an audio codec for telephony in the North American region
112 Authority	The national/regional/local authority responsible for overall operation of, and data for the 112 system
AdditionalAgency Event	A log entry indicating another agency's involvement with a call or incident, which may have log records for that call or event in their own log.
Additional Data	Data associated with a call for which a URI is sent with the call or retrieved from the ECRF, for example, Additional Call Data, Additional Caller data and Additional Location Data
Agency Identifier	A domain name for an agency used as a globally unique identifier.
Authentication	A security term referring to the process of reliably identifying an entity requesting access to data or a service.
Authorization	A security term referring to the process of making a decision what access rights an authenticated entity has to data or a service
B2BUA	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.
Bridging	Connecting two or more parties with a conference bridge
BYE transaction	A SIP transaction used to terminate a session
Call	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-associated 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. 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 NG112.
Call Detail Record (CDR)	A record stored in a database recording the details of a received or transmitted call
Call Identifier	An identifier assigned by the first element in the first ESInet which handles a call. Call Identifiers are globally unique.

Term	*Definition*
Call-Info Header	A SIP header which contains a URI referring to some kind of data relevant to a call, and a "purpose" parameter describing what the URI refers to. Used to carry URIs to such entities as Additional Call and Caller data, and call/Incident Tracking Identifiers
CANCEL transaction	A SIP transaction which is used to cancel an INVITE transaction which has not yet completed
CAP MESSAGE	A notification using the Common Alerting Protocol. CAP is used within the ESInet to send alerts from automated systems to PSAPs, and is also used to communicate data between agencies without a call.
Catypes	A component of a civic address in a PIDF-LO such as a Street Name or House Number, which has a code used to identify what kind of component.
Code Point	A code for a requested QoS action used in the Diffserv QoS mechanism on an IP network. The code point is sent in the TOS field of an IP packet.
Denial of Service Attack	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.
Dereference	The act of exchanging a reference to an item by its value. Used primarily with a Location URI. The dereference operation uses a protocol such as SIP or HELD to obtain a location value (PIDF-LO).
Diffserv	A quality of service mechanism for IP networks characterized by a code in a field of a Packet called a "Code Point" and a "Per hop Behavior"
Domain (or Domain Name)	The domain name (hostname) of an agency or element in an ESInet. See Domain Name System (DNS)
Element Identifier	A logical name used to represent physical implementation of a functional element or set of functional elements as a single addressable unit. The form of an element identifier is a hostname.
Emergency Call Routing Function (ECRF)	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.

Term	Definition
Emergency Event	An asynchronous communications notification which is a single communication message to a PSAP that results in a defined action by a call taker but does not have a human at the origination end and where no two way media streams are established.
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 functional processes can be deployed, including, but not restricted to, those necessary for providing NG112 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).
From Header	A SIP header that describes the caller's notion of its own identity (Address of Record). From is generally not treated as reliable unless it is protected by an Identity header
geoShape Element	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
H.264	A video codec, defined by ITU-T in common use today for real time two way video
HELD	A protocol defined by the IETF to deliver location using HTTP transport
IANA Registry	A registry maintained by the Internet Assigned Number Authority, usually at the behest of the IETF
Incident	A real world occurrence such as a heart attack, car crash or a building fire for which one or more calls may be received.
Incident Tracking Identifier	An identifier assigned by the first element which declares an incident. Incident Tracking Identifiers are globally unique.
INFO	A SIP transaction used to pass information from the caller to the called party
Instant Messaging (IM)	A method of communication generally using text where more than a character at a time is sent between parties nearly instantaneously
INVITE	A SIP transaction used to initiate a session
Legacy PSAP Gateway	An NG112 Functional Element which provides an interface between an ESInet and an un-upgraded PSAP

Term	*Definition*
Location	In the context of location information to support IP-based emergency services: The physical position of an end-point expressed in either civic or geodetic form. A spot on the planet where something is; a particular place or position. Oxford Dictionary, Oxford University Press, 2009.
Location Interwork Function (LIF)	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.
Location URI	A URI which, when dereferenced, yields a location value in the form of a PIDF-LO. Location-by-reference in NG112 is represented by a Location URI.
Mapping	The act of determining a value in one domain from a value in another domain. For example, mapping a location to the URI of a PSAP that serves that location using the LoST protocol.
MESSAGE	A SIP method which passes information, often an Instant Message, between endpoints in the body of the SIP message
NG112 Specific Interwork Function (NIF)	The functional component of a Legacy Network Gateway or Legacy PSAP Gateway which provides NG112-specific processing of the call not provided by an off-the-shelf protocol interwork gateway.
Next Hop	The next element in a routing path. For example, the next router in an IP network, or the next SIP proxy server in a SIP signaling path.
Non-human-initiated	A term for calls originating from automated sensor-based devices (e.g., alarm systems) where there is no assumption of a human presence. Non-human-associated calls are non-interactive and normally do not create SIP sessions. Such calls contain data and may include URIs or information for contacting a human, viewing streaming meda, controlling a device, etc.
Notifier	An element in an asynchronous event notification mechanism that transmits events
NOTIFY	A SIP method used to send a notification to a subscriber of the occurrence of an asynchronous event.

Term	Definition
OPTIONS	A SIP method used to request the SIP protocol options supported by an endpoint.
Originating ESRP	The first routing element inside the ESInet. It receives calls from the BCF at the edge of the ESInet.
Per Hop Behaviors (PHB)	The action a router takes for a packet marked with a specific code point in the Diffserv QoS mechanism in IP networks
Policy Routing Function (PRF)	That functional component of an Emergency Services Routing Proxy that determines the next hop in the SIP signaling path using the policy of the nominal next element determined by querying the ECRF with the location of the caller.
Policy Store	A functional element in the ESInet that stores policy documents.
PRACK	A SIP message used to reliably acknowledge receipt of an otherwise unreliable message transmission.
Protocol Interworking Function (PIF)	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.
Provisioning Service provider (PSP)	The component in an ESInet functional element that implements the provider side of a SPML interface used for provisioning
PSAP Credentialing Agency (PCA)	The root authority designated to issue and revoke security credentials (in the form of an X.509 certificate) to authorized 112 agencies in an ESInet.
Real Time Text (RTT)	Text transmission that is character at a time, as in text phones.
REFER	A SIP method that is used as part of a transfer operation to refer a call to another endpoint
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.
REGISTER	A SIP method that is used to communicate the availability and address of an endpoint to the proxy server that directs incoming calls.
reINVITE	A SIP INVITE transaction within an established session used to change the parameters of a call.
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.

Term	*Definition*
Resource Priority	A header used on SIP calls to indicate priority that proxy servers give to specific calls.
ReverseGeocode	The process of converting a geo form of location (X,Y) to a civic (street address) form.
Rights Management	Specifying the access rights by an entity (agent or agency) to a particular document, data element, or service
Scheme	The part of a URI that indicates the protocol. For example, the scheme in the URI sip:john@example.com is "sip"
Security Posture	An event that represents a downstream entity's current security state (normal, under attack, …).
Service Boundary	A polygon in a GIS system, SIF, ECRF or other ESInet element that indicates the area a particular agency or element serves.
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 consider when determining a response. A service URN is also used to mark a call as an emergency call.
Session Border Control	A commonly available functional element that provides security, NAT traversal, protocol repair and other functions to VoIP signaling such as SIP. A component of a Border Control Function
Smart Cards	A credit-card-like object that contains a processor and memory, and is typically used to carry credentials for an agent in an authentication system. A smart card may be one factor in a 2 or 3 factor authentication system and is "something you have"
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.
SUBSCRIBE/NOTIFY	The two actions in an asynchronous event notification system. The subscription is the request to receive notifications of the events. The Notify is the notification of the event itself. Also refers to the SIP methods used for this purpose.
Subscriber Database (SDB)	A database operated by a carrier or other service provider which supplies the "Additional Call" data object. The SDB dereferences the URI passed in a Call-Info header and returns the AdditionalCall XML object.
SubjectAltName	A field in an X.509c digital certificate which typically contains identifying information for the entity issued the certificate. In an ESInet, SubjectAltName contains an agent or agency ID

Term	*Definition*
Terminating ERSP	The last ESRP for a call in an ESInet, and typically chooses a queue of call takers to answer the call
Token	A physical device that displays a multidigit number used as part of an authentication system ("something you have"). Also, a set of bits that represent some data, permission or state which is meaningful to the recipient, but not necessarily the sender.
Transcoding	Translating a media stream from one codec to another. For example, translating text telephone modem tones detected in a G.711 encoded audio stream to T.140 real time text
UPDATE	A SIP method used to update parameters in a call not yet established

4 Functional Elements

This section describes the functional elements in the NG112 architecture, as shown in Figure 1.

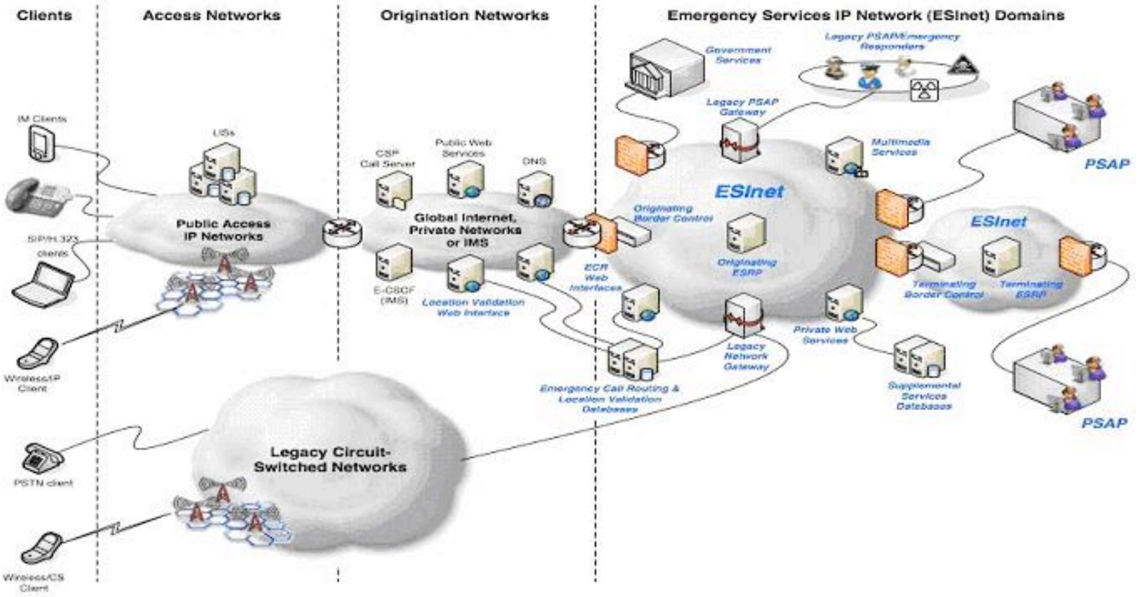

Clients
Access Networks
Origination Networks
Emergency Services IP Network (ESInet) Domains
IM Clients
SIP/H.323 clients
Wireless/IP Client
PSTN client
Wireless/CS Client
LISs
Public Access IP Networks
Legacy Circuit-Switched Networks
CSP Call Server
Public Web Services
DNS
Global Internet, Private Networks or IMS
E-CSCF (IMS)
Location Validation Web Interface
ECR Web Interfaces
Emergency Call Routing & Location Validation Databases
Government Services
Legacy PSAP/Emergency Responders
Legacy PSAP Gateway
Multimedia Services
ESInet
Originating Border Control
Originating ESRP
Legacy Network Gateway
Private Web Services
Supplemental Services Databases
ESInet
Terminating Border Control
Terminating ESRP
PSAP
PSAP

Figure 1: NG112 High Level Architecture.

The left side of the picture shows various originating networks with a range of devices being able to trigger emergency communication. The originating networks include over-the-top VoIP provider, IMS operators, enterprise networks, as well as legacy circuit switched networks. The standardization of the communication of the left-side of the figure is largely outside the scope of this specification although proper integration of IP-based emergency services functionality helps to ensure correct functioning of the emergency services functionality.

The bulk of the description found in this document concerns the right side of the figure denote as the "Emergency Services IP Network (ESInet) Domains". The ESInet is an emergency services network that utilizes IP technology to perform emergency call routing and related functionality. The borders of the ESInet are secured using network level firewalls, and application layer firewalls (so-called Border Control Functions – BCFs). These devices are used to authorize every IP-based communication attempt entering the ESINet. For interworking with legacy technology Legacy Network Gateways (LNGs) are utilized. In addition to their security function they also perform protocol translation from and to IP-based SIP signaling, and IP-based data exchange.

Location information is a crutial aspect for the ESInet in two ways.

1. First, the Emergency Services Routing Proxy (ESRP) is a SIP entity that makes decisions about the call routing and uses location information for that purpose. Location is, however, not the only information used to determine call routing. Overload situations at PSAPs, time of day, skills of call takers, available technological features at the PSAPs, special needs of the emergency callers, etc. may influence call routing.
2. Second, precise location information is also needed to dispatch first responders.

For this purpose various ESInet components need access to the caller's location information. In NG112, location information may be provided with the call, or accessed during the call by use of a reference to location information.

However, not all ESRPs need to be equipped with the logic to perform complex policy based call routing decisions. Instead, the classical separation between a Policy Enforcement Point (PEP) and a Policy Decision Point (PDP) is utilized by allowing the ESRP to act as a PEP and to outsource the decising making to the Emergency Call Routing Function (ECRF). To decision of the ECRF can be cached by the ESRP for performance and resilience reasons (as long as indicated by the provided expiry time).

The most important component in the ESInet are the PSAPs, which are used by call takers to interact with the emergency caller.

The sub-sections below provide additional details about the listed functional elements as well as associated elements.

4.1 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. The ESInet has a service area, defined by a (set of) polygon(s). 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.

This document does not mandate how large these networks are nor who operates them. These operational aspects are likely to vary over time and from country to country.

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.

The ESInet must be connected to the Internet through the Border Control Function (BCF) to accept calls. This Internet interconnect is recommended at the state ESInet level. 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 VPN.

Access to ESInets must be controlled. Only public safety agencies, their contractors and service providers should be connected directly to the ESInet. 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). 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 and Per Hop Behaviors (PHB) must be used on ESInets:

DSCP	**Use**	**PHB**
0	Routine Traffic	Default
1	112 Signaling	AF12
2	112 Text Media	AF12
3	112 Audio Media	EF
4	112 Video Media	AF11
5	112 Non-human-associated Call	AF21
6	Intra ESInet Events	AF21
7	Intra ESInet Other 112 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 in globally reachable DNS servers. Use of statically assigned IP addresses should be limited, and should never be used with IPv6 addresses. DHCP must be implemented on all network elements to obtain IP address, gateway, and other services. Many ESInet services depend on discovery of services via DHCP.

There must be no single point of failure for any critical service or function 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.

4.2 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.

4.2.1 Functional Description

The Border Control Function 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 border control function support the following security related techniques:

- Prevention
- Detection
- Reaction

Additionally, the entirety of the functional element may include aspects of the following:

- 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 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 Internet originated malware attacks that are protocol specific.

2) Network layer — these manage access on the Internet 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., 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) attack, 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 Public Safety Computer Emergency Response Team (CERT) or other managing authority
4) Capability to receive and update 112 Malicious Content (NMC) filtering automatically for use by federated firewalls in protecting multiple disparate ESInets
5) Adhere to the default deny principle.

Note that NENA 04-503 [102] provides some information on firewall configuration requirements.

Session Border Control — The session border controller functional element of the BCF plays a role in VoIP services by controlling borders to resolve multiple VoIP-related problems such as Network Address Translation (NAT) or firewall traversal. Session Border Controllers (SBCs) are already being extensively used in existing VoIP service 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 BCF, 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)
- Protection against DDoS attacks: The SBC component of the BCF shall protect against VoIP specific and general DDoS attacks on VoIP network elements.
- 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 NAPT Traversal: The SBC component of the BCF shall perform NAT traversal for authorized calls/sessions using SIP protocol. The SBC component attempts to recognize that a NAT or NAPT has been performed to 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 BCF 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 BCF 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 Back-to-Back User Agent 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., 112 calls) in order to facilitate priority routing of the packets.
- Call Detail Recording - The SBC component of the SBC 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 SLA auditing.
- Transcoding: The SBC component of the BCF shall optionally support transcoding. For example, the SBC component may transcode between PSTN text telephone tones and RFC4103 real time text. In other cases transcoding between G.711 and G.729 and DTMF interworking may be required. See Section 5.1.8.3.

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.

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

- Encryption and decryption of media.

B2BUA for UAs that do not support Replaces

- The SBC component may include a B2BUA function for 112 calls where the caller does not indicate support for the Replaces operation. See section 4.9.1.

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.

4.2.2 Interface Description

The BCF supports SIP interfaces upstream and downstream per Section 5.1. BCFs must support ROHC [145]. 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 "EES-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 EES-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 EES-source parameter that was included in the Via header of the incoming INVITE message. The BCF responds by returning a BadActorResponse message, which 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.

The bad actor report is a webservice operated on the domain mentioned in the parameter.

BadActorRequest

Parameter	Condition	Description
sourceId	Mandatory	sourceId from a EES-source parameter

BadActorResponse

Parameter	Condition	Description
errorCode	Mandatory	Error Code

Error Codes

100	Okay No error
101	Already reported
512	No such sourceId
513	Unauthorized
504	Unspecified Error

4.2.2.1 Suspicious Calls

The BCF may be able to identify calls that may be part of a deliberate attack on the system. However, under normal conditions, we 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 the Spam-Scope header to the SIP message. The Spam-Score header syntax and semantic is defined in [155]. How the BCF computes the values for suspicious calls is outside the scope of this document, similar to how spam marking in emails works.

4.2.3 Roles and Responsibilities

The ESInet operator is responsible for the BCF at the edge of the ESInet. PSAP or other agency is responsible for a BCF between its network and the ESInet.

4.2.4 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 edition, 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.

4.3 Emergency Service Routing Proxy (ESRP)

4.3.1 Functional Description

4.3.1.1 Overview

The Emergency Service Routing Proxy (ESRP) is the base routing function for emergency calls, 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 a PSAP, just past 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 112 calls received by an ESRP it;

1. Evaluates a policy "rule set" for the queue the call arrives on
2. Queries the location-based routing function (ECRF) with the location included with the call to determine the "normal" next hop (smaller political or network subdivision, PSAP or call taker group) URI.
3. Evaluate a 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 above).

The ESRP may also handle calls to what used to be called "administrative lines," meaning calls directed to a E.164 number listed for a particular PSAP. 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 112 calls. Such calls would not have a Geolocation header and the ESRP would not query an ECRF, but would use the E.164 number to map to a PSAP URI (the same URI which the ECRF would yield), and use that URI as the "normal next hop" used to select the policy rule set to evaluate.

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. Callbacks 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.

4.3.1.2 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 managed by an ESRP. A call sent to the queue URI must route to the ESRP 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 are dequeued by the ESRP sending the call to a downstream entity (ESRP or endpoint such as a call taker or IMR).

ESRPs may, and often will, manage multiple queues. For example, an ESRP may manage a queue that is used for normal 112 calls routed to the local ESInet, and one or more queues for calls that are diverted to it by ESRPs from other areas, which 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 making simple routing decisions per RFC3264. 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 policy that controls which entities may enqueue and dequeue calls to the queue. The dequeueing entity registers (DequeueRegistration) to receive calls from the queue. The ESRP would return a call from an entity not in its policy with a 404 error.

The ESRP will maintain a QueueState notifier, and track the number of calls in queue for the queues that it manages.

4.3.1.3 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 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: EES-QueueState

Event Package Parameters: None

SUBSCRIBE Bodies: standard RFC4661 + extensions filter specification may be present

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

NOTIFY Bodies: MIME type application/vnd,EES.queuestate+xml

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 [113]. 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 are 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, we ensure relatively frequent NOTIFYs of the QueueState event. Successful completion of the NOTIFY is indication to the upstream entity that calls sent to the downstream entity should succeed. The subscription may include a "force" and/or "throttle" filter [113] to control the rate of Notification.

4.3.1.4 DequeueRegistration Event Package

DequeueRegistration is 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. The registration includes a value for DequeuePreference, which 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
dequeuePreference	Optional	Integer from 1-5 indicating queuing preference.

DequeueRegistrationResponse

Parameter	**Condition**	**Description**
errorCode	Optional	Error Code

Error Codes

100	Okay No error
506	Bad queue
507	Bad dequeuePreference
508	Policy Violation
504	Unspecified Error

The ESRP will subscribe to the QueueState event for each dequeueing entity to determine its availability to take calls. Normally, a dequeueing entity is another queue maintained at the downstream entity, although the queue maintained at the terminating ESRP, which is normally the PSAP, would use call taker state rather than queue state to determine availability to dequeue calls from its upstream ESRP.

4.3.1.5 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 rulesets: one set determined by the queue the call arrives on, the other 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 ruleset. The rules normally include at least one action LoSTServiceURN (<urn>) where urn is a service urn (either urn:service:… or urn:EES:service:…). Upon encountering the LoSTServiceURN action, the PRF queries its (configured) ECRF with the location received in the call using the urn parameter in the action. The resulting URI is a variable called "NormalNextHop". The PRF extracts a "TerminationPolicy" from its policy store associated with the domain of NormalNextHop and executes the ruleset 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 112 call intended for a PSAP in a normal state to be identical to the "NormalNextHop" URI, that is, if the ECRF query returned sip:psap1@example.com, then the TerminationPolicy ruleset for sip:psap1@example.com would have a Route (sip:psap@example.com) or a Route (NormalNextHop), 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 NormalNextHop 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 routes to an Interactive Multimedia Response system, conforming to RFC4240 [43], that plays an announcement (in the media negotiated by the caller) and potentially accepts responses via DTMF, KPML or other interaction styles.

The syntax is Route (<recipient>, <cause>), where recipient is a URI which will become the Request URI for the outgoing SIP message, and the <cause> is a value used with the Reason header associated with a History-Info header. The <cause> values are defined in a Registry, which this document establishes.

Other Actions that may occur in a Termination-Policy include:

- Busy() which returns 600 Busy Everywhere to the caller
- Notify(<recipient>, <eventCode>,<urgency>, <severity>,<certainty>), which sends a NOTIFY 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.

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 ruleset.

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

1. ElementState, 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 that of a PSAP that the ESRP can subscribe to the ElementState package for.
2. QueueState (and implied "Not Reachable" state), expressed as QueueState.<queue> where <queue> is the name of a queue
3. SecurityPosture, expressed as SecurityPosture.<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 an agency or element that the ESRP can subscribe to the SecurityPosture package for.
4. CallSuspicion, the BCF's opinion of the call, expressed as CallSuspicion.<suspicionLevel>.
5. Call Source (as defined in the Via headers of the INVITE), 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 SP prior to the ESInet should be returned. If there are no originating networks, CallSource returns the domain of the caller.
6. Any header in the call INVITE message, expressed as Invite.<header name>. Even though a call may be initiated with a sip Message, Invite.<header name> is used to specify the headers
7. 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.
8. The location used for routing, expressed as PIDF.<element name>
9. Any element in the Additional Data about a call or caller or location structures if available, expressed as AcallData.<element name>, AcallerData.<element name> or AlocationData.<element name>. See Sections 4.11 and Section 8.

10. Time of Day, expressed as TimeOfDay or DayOfWeek, where TimeOfDay is wall clock time (0000 to 2359) and DayOfWeek is Mon, Tue, Wed, Thu, Fri, Sat, Sun.
11. RequestURI (URI call was sent to ESRP with)
12. ECRF query results (Normal-NextHop).
13. The queue the call was received on (IncomingQueue)

Rules have a priority. If more than one rule yields a value for NextHop, the rule with the highest priority prevails. If more than one rule with the same priority yields a value for NextHop, the ESRP chooses randomly from the results with approximately uniform distribution.

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(NormalNextHop) {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 NG112 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 become a dequeuer for one or more upstream queues. 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 ruleset is used). In such a case, the origination policy ruleset would determine NextHop. Rules can determine the priority of multiple queues feeding calls to the ESRP. PSAP ESRPs may dequeue for multiple call queues, placing them on internal queues for call takers.

4.3.1.6 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 AdditionalCallData record may have a telematics dataset that indicates a severe injury. The ruleset 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: EES-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 RFC4661 + extensions. Filter specification may be present

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

NOTIFY Bodies: MIME type application/vnd,EES.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 Geolocation header must also be copied to the NOTIFY headers. The CAP message is in the body of the NOTIFY, with MIME type **application/common-alerting-protocol+xml.**

A list of the parameters on the notification will be provided in a future edition of this document

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 "EES-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 13.5. 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.

If there are Call-Info headers containing Additional Data (Call or Caller), they must be sent in the CAP message in a <parameter> element. Additional Call data has a <value name> of ADDLCALL and Additional Caller data has a <value name> of ADDLCALLR. The URI is 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.

The CAP message may be enclosed in an EDXL wrapper. If it is, 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 [113] may be used to limit Notifications.

State Agents: No special handling is required.

4.3.1.7 Processing of an INVITE transaction

When the ESRP receives an INVITE transaction it first evaluates the Origination ruleset for the queue the call arrived on. If a LoSTServiceURN action 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 source IP address of the call 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 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 Route header in the LoSTServiceURN action 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:EES: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 ruleset for the URI. The PRF evaluates the ruleset 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 evaluate 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. If no entity responds, 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 report their state to the ESRP and the ruleset 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.

4.3.1.8 Processing a BYE Transaction

An ESRP processes BYEs per RFC 3261.

4.3.1.9 Processing a CANCEL transaction

An ESRP processes CANCELs per RFC 3261.

Note: *The ESRP should have a way to notify a PSAP that a call arrived at the ESRP, but was CANCELled before the INVITE was sent to the PSAP. This would be one case of abandoned call. This will be covered in a future edition of this standard.*

4.3.1.10 Processing an OPTIONS transaction

An ESRP processes OPTIONS transactions per RFC3261. The OPTIONS method is often used as a "keep alive" mechanism. During periods of inactivity, the ESRP should periodically send OPTIONS towards its upstream entities and expect to see OPTIONS transactions from its downstream dequeueing entities.

4.3.2 Interface Description

4.3.2.1 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. The upstream SIP call interface for the originating ESRP must only assume the minimal methods and headers as define in Section 5.1.1 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. The ESRP must assure that pager mode Instant Messages route to the same PSAP per Section 5.1.9

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 callbacks) 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.

4.3.2.2 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 5.1.2 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 may include a Route header. The Request URI remains urn:service:sos (although the ESRP may not depend on that) and it replaces the top Route header with the next hop URI (this is described in [59]). The ESRP adds a History-Info and Reason headers per Section 5.1.7 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 with a purpose parameter of "EES-IncidentId" and a new Incident Tracking Identifier. The ESRP also creates a new

Call identifier and adds a Call-Info header with a purpose parameter of "EES-CallId".

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.

4.3.2.3 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.

The ESRP must use the ECRF interface with the "urn:EES:service:AdditionalLocationData" service URN when the relevant ruleset specifies an element in that structure. The same location used for the location-based route is used for the AdditionalLocationData query.

4.3.2.4 LIS Dereference Interface

The ESRP must implement both SIP Presence Event Package and HELD dereference interfaces. When the ESRP receives a location (in a Geolocation header on the upstream SIP interface) it uses the LIS dereference interface to obtain a location value to use in its ECRF query. The ESRP uses its PCA issued credentials to authenticate to the LIS[1]. The ESRP must use TCP/TLS for the LIS Dereference 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.

4.3.2.5 Additional Data Interfaces

The ESRP must implement an https client in order to support the AdditionalCallData services. These services may be invoked when the ESRP receives a call with a CallInfo [12] header with a "purpose" of "emergencyCallData",

[1] 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.

“emergencyCallerData” or “emergencyPSAPdata”. These services may attempt to resolve the HTTPS URIs present in AdditionalCallData headers. Resolving such URIs results in an XML data structure. These data structures are used as input to the Policy Routing Function. The ESRP must be able to accommodate multiple additional data services and structures for the same call.

Note: Multiple CallInfo headers with "emergencyCallData" 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. The call may have more than one Call-Info header with emergencyCallerData when, for example, the call is from a residence wireline telephony service where there is more than one resident. When used in a routing rule, the PRF merges multiple AdditionalCall or AdditionalCaller data. If the merge results in conflicting information, the information derived from earlier-encountered Call-Info headers shall take precedence over information derived from subsequent Call-Info headers.

The ESRP should only invoke the web service when the relevant ruleset specifies an input from an AdditionalCallData/AdditionalCallerData/AdditionalPSAPdata structure.

The ESRP must also be able to query the ECRF for AdditionalLocationData when the policy rules are dependent on that data.

The ESRP must support both CID and HTTPS URIs.

4.3.2.6 ESRP, PSAP and Call Taker State Notification and Subscriptions

The ESRP must implement the client side of the ElementState event notification packages. The ESRP must maintain Subscriptions for this package on every downstream element 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, which affects its ability to receive calls, must be reported.

4.3.2.7 Time Interface

The ESRP must implement an NTP client interface for time-of-day information. The ESRP may also provide an interface to a hardware clock. The time of day information is an input to the Policy Routing Function as well as the logging interface

4.3.2.8 Logging Interface

The ESRP must implement a logging interface 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 ruleset it consulted, the rules found to be relevant to the route, and the route decision it made.

Note: *The specifics of the log entries will be provided in a future edition of this document.*

4.3.3 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 queue, including the states of the entities registered to dequeue calls from the queue, the overall queue state, the number of calls in queue, the max number of calls allowed, and the current queue state.

The ESRP constructs AdditionalCallData, AdditionalCallerData and AdditionalLocationData structures when the relevant ruleset mentions elements from these structures and, in the case of call and caller data, the upstream Call Interface receives the appropriate CallInfo header with a URI for the AdditionalCallData/AdditionalCallerData dereferencing services.

4.3.4 Policy Elements

The ESRP uses an Origination-Policy ruleset for each queue it manages. For every URI the ECRF can return for the service query the ESRP makes (Normal-NextHop), it must have access to the appropriate Termination-Policy ruleset.

The ESRProuteEvent Policy determines which entities may subscribe to the ESRProute Event.

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

The takeCallsOnQueues policy determines which queues this ESRP will dequeue from (that is, which queues it will subscribe to the dequeueRegistration and queueState events for)

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

4.3.5 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 E.164 PSAP telephone numbers to URIs (if the ESRP handles calls made to E.164 numbers on behalf of PSAPs)
- The URI of a default route PSAP that takes calls when a route cannot be determined.

4.3.6 Roles and Responsibilities

An ESRP may be operated by a State, Regional or local 112 authority. A terminating ESRP may be operated by a PSAP. The ESRP for non-originating ESRPs must supply a ruleset for the upstream ESRP.

4.3.7 Operational Considerations

To be provided in a future edition of this standard.

4.4 Emergency Call Routing Function (ECRF)

In NG112, emergency calls will be routed to the appropriate PSAP based on the location of the caller. In addition, PSAPs may utilize the same routing functionality to determine how to route emergency calls to the correct responder. The NG112 functional element responsible for providing routing information to the various querying entities is the Emergency Call Routing Function (ECRF). An ECRF provided by a 112 Authority and accessible from outside the ESInet must permit querying by an IP client/endpoint, an IP routing proxy belonging to a VSP, a Legacy Network Gateway, an Emergency Services Routing Proxy (ESRP) in a next generation Emergency Services network, or by some combination of these. An ECRF accessible inside an ESInet must permit querying from any entity inside the ESInet. ECRFs provided by other entities may have their own policies on who may query them. An origination network may use 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, to the correct ESInet for the emergency call. The ECRF must be used within the ESInet to route calls to the correct PSAP, and by the PSAP to route calls to the correct responders.

4.4.1 Functional Description

The ECRF 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. 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 to the PSAP itself. 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 might identify a secondary agency.

4.4.2 Interface Description

4.4.2.1 Routing Query Interface

The ECRF shall support a routing query interface that can be used by an endpoint, ESRP, or PSAP to request location-based routing information from the ECRF. The ECRF takes the location information and Service URN received in a routing query and maps it to the destination URI for the call. The LoST protocol supports this functional interface in NG112.

When an ECRF receives a LoST query, the ECRF determines whether an authenticated user (e.g., an ESRP) originated the query and the type of service requested (i.e., emergency services). Authentication must apply for ESRPs and PSAPs that initiate queries to the ECRF. TLS is used by all ECRFs within the ESInet, and credentials issued to the entity querying 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 should assume a common public identity for such queries. Based on the identity and credentials of the query originator and the service requested, the ECRF determines which URI is returned in the LoST response, which could be a URI of a PSAP or a downstream ESRP. The same database used to route a call to the correct PSAP may also be used to subsequently route the call to the correct responder, e.g., to support selective transfer capabilities.

The LoST protocol is a query/response protocol defined by [61]. The client seeking routing information sends a LoST <findService> query to the server (in this case the ECRF). The ECRF responds to the query with a response message that contains the requested information (see <findServiceResponse> in Section 5.5.1.1.2), an error indication (see <errors> in Section 5.5.1.1.3), or a redirect to another ECRF (see <redirect> in Section 5.5.1.1.4). The LoST protocol is a flexible protocol and is defined with many options. Many of the options provided in the LoST protocol are not specifically required to support emergency call routing.

4.4.2.1.1 Routing Query

The LoST protocol specifies the following query messages:

- <findService>
- <getServiceBoundary>
- <listServices>
- <listServicesByLocation>

The <findService> message is used to retrieve one or more contact URIs given a service URN and a location. Since the primary function of the ECRF is to support the routing of emergency calls, the ECRF must be capable of receiving, processing and responding to LoST <findService> query messages containing the "sos" service or a "sos" sub-service URN. See Section 5.5.1.1.1 for an explanation of the LoST <findService> message. 112 Authorities may also choose to route other sos urns to the primary PSAP.

The ECRF may also support the other LoST query types (see [61] for details related to the <getServiceBoundary>, <listServices>, and <listServicesByLocation> query messages).

4.4.2.1.2 Routing Response

The LoST protocol describes the following response messages that can be used depending on the received query:

- <findServiceResponse>
- <findServiceBoundaryResponse>
- <listServicesResponse>
- <listServicesByLocationResponse>

The only response message that the ECRF is required to support is the <findServiceResponse> message. The ECRF shall be capable of generating a LoST <findServiceResponse> message (Section 5.5.1.1.2) an <errors> message (Section 5.5.1.1.3), or a <redirect> message (Section 5.5.1.1.4) in response to a received <findService> message.

The <findServiceResponse> message is composed of the elements listed in Table 4-2.

Table 4-2. <findServiceResponse> Message Elements

Element	Condition	Description
source	Mandatory	Identifies the authoritative generator of the mapping
sourceId	Mandatory	Identifies a particular mapping
lastUpdated	Mandatory	Describes when a mapping identified by the source and sourceId was last updated
expires	Mandatory	Identifies the absolute time when the mapping becomes invalid

<displayName>	Optional	Describes a human readable display name, e.g., the name of the PSAP serving the location
<service>	Mandatory	Identifies the service for which the mapping applies
<serviceBoundary>	Optional	Identifies the area where the URI returned would be valid
<serviceBoundaryReference>	Optional	Identifies the reference which could be used to access the service boundary for which the URI returned is valid
<serviceNumber>	Optional	Provides the emergency services dial string that is appropriate for the location provided in the query
<uri>	Conditional[2]	Contains the appropriate contact URI for the service being requested
<path>	Mandatory	Contains the Via elements indicating the LoST servers that handled the request. Used for recursive operation.
<locationUsed>	Optional	Identifies the location used to determine the URI

[2] The ECRF shall include a URI in a <findServiceResponse> message if one can be determined.

<locationValidation>	Optional	Indicates which elements of the civic location were "valid" and used for mapping, which elements were "invalid" and which elements were "unchecked"

The elements that make up the <findServiceResponse> message are described below:

- source - This element identifies the authoritative generator of the mapping (the LoST server that generated the mapping). LoST servers are identified by U-NAPTR/DDDS application unique strings, in the form of DNS name. For example, lostserver.notreal.com.
- sourceId - This element identifies a particular mapping at the LoST server and is unique among all the mappings maintained by the LoST server.
- lastUpdated - This element describes the date and time when this specific instance of mapping was updated. The date and time is represented in UTC format.
- expires - This element describes the date and time when a particular mapping becomes obsolete. The date and time are described using a timezoned XML type datetime. This element may optionally contain the values of "NO-CACHE" indicating that the mapping should not be cached and "NO-EXPIRATION" indicating that the mapping has no expiration instead of the date and time.
- <displayName> Element - The display name 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.
- <service> Element - The <service> element identifies the service for which this mapping is valid. The ECRF is required to support the sos service. Support for other services will depend on local implementation.
- <serviceBoundary> - The <serviceBoundary> element identifies the geographical area where the returned mapping is valid. The intent of this parameter is to allow a mobile endpoint to realize that it is moved out of the area where a stored mapping is valid and trigger it to query for a new valid mapping. This element may be supported by the ECRF depending on local implementation.
- <serviceBoundaryReference> - The <serviceBoundaryReference> element identifies a reference that could be used to access the service boundary for

the requested mapping. This parameter may be supported by the ECRF depending on local implementation.

- <serviceNumber> - The <serviceNumber> element contains the emergency services number that is appropriate for the location provided in the query. This will allow a foreign end device to recognize that an emergency number is being dialed.
- Uniform Resource Identifier (<uri>) - The <uri> specifies either the address of the PSAP or the ESRP that is appropriate for the location sent in the query message. The decision of whether to send the PSAP <uri> or the ESRP <uri> is based on whether the query is made by the end user, VSP Routing Proxy, NG112 PSAP, or the ESRP. In this architecture, the end point and VSP Routing Proxy will receive an ESRP <uri>. Only authorized ESRPs and NG112 PSAPs are entitled to receive a PSAP <uri>. Lower layer authorization procedures are used to identify the query originator.
- <path> - The <path> contains via elements indicating the ECRF(s) that handled the request.
- <locationUsed> - The <locationUsed> element identifies the location used to determine the URI.
- <locationValidation> - The <locationValidation> element identifies which elements of the received civic address were "valid" and used for mapping, which were "invalid" and which were unchecked. Since the ECRF is not responsible for performing validation, this parameter may not be returned, subject to local implementations.

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 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, two <mapping>s 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 service boundary returned from an ECRF may not be the actual service boundary of the PSAP, or even that of the ESRP that will handle an emergency call from the location in the query. Instead, it may be a simpler shape chosen to have only a few points. For example, the polygon may be the largest rectangle that completely fits in the actual boundary measured from the location in the query. The service boundary returned at a point near a service boundary may represent a portion of the agency's service boundary near the edge where the location exited the original boundary, and may be somewhat more complex, but still an approximation of the actual boundary. As the location sent in the query gets closer and closer to the actual service boundary, the area represented by the returned service boundary may be smaller, the number of points may be somewhat larger, and the fidelity to the actual service boundary may be greater. This minimizes the network bandwidth and compute load on the device.

4.4.2.1.3Error and Warning Messages

If the ECRF is unable to completely fulfill a request, it shall return either an error or a warning message, depending on the severity of the problem.

If no useful response can be returned for the query, the ECRF shall return a LoST <errors> message with the appropriate "error type" element(s) as described in Section 5.5.1.1.3 and Section 13.1 of [61].

If the ECRF is able to respond to a query in part, it shall return a <warnings> element as part of another response element as described in Section 13.2 of [61] and in Section 5.5.1.1.3 for the Lost <findServiceResponse> message.

In both cases, the source attribute of the "error type" and "warning type" element(s) identifies the server that originally generated the error or warning (e.g., the authoritative server). When possible, the ECRF should populate the message and xml:lang attributes of the "warning type" and "error type" elements to more specifically identify the nature of the warning or error for logging and possible later troubleshooting purposes.

4.4.2.2 Data Source Interface

The ECRF's data source is a map, specifically, a set of layers from one or more source SIFs (Spacial Information Function). A SIF layer replication interface is used to maintain copies of the required layers. The ECRF is provisioned with the URI and layer names of its data sources. It has layers that define the locations (state/county/municipality/street/address), as well as service boundary polygons.

A resulting location-based URI associated with a routing request may undergo further modification at an ESRP due to policies related to such things as time of day, current congestion conditions, etc. (See Section 4.2.4 for further discussion.)

4.4.2.3 Time Interface

The ECRF must implement an NTP client interface for time-of-day information. The ECRF may also provide an interface to a hardware clock. The time of day information is an input to the mapping expiration time as well as the logging interface.

4.4.3 Data Structures

4.4.3.1 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 SIF 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.

The ECRF shall be capable of receiving the following data elements that may be present in the civic location information received in a routing query from an NG112 element (i.e., VoIP endpoint, VSP Routing Proxy, ESRP, PSAP), identifying the service boundary the civic location described by the data elements lies within, and performing a mapping to determine the associated routing data. RFC 4776 ([8]) provides a full set of parameters that may be used to describe a civic location. Specifically, RFC 5139 ([76]) lists several civic address types (CAtypes) that require support in the formal PIDF-LO definition that are not in RFC 4119 ([6]).

Table 4-3. Civic Location Data Elements

Label	**Description**	**Type**
country	2-letter ISO code	alphanumeric
A1	national subdivision (e.g., state)	alphanumeric
A2	county, parish	alphanumeric
A3	city, township	alphanumeric
A4	city division, borough	alphanumeric

A5	neighborhood	alphanumeric
A6[3]	street	alphanumeric
PRD	leading street direction	alphanumeric
POD	trailing street suffix	alphanumeric
STS	street suffix	alphanumeric
HNO	house number	alphanumeric
HNS	house number suffix	alphanumeric
LMK	Landmark or vanity address	alphanumeric
LOC	additional location info	alphanumeric
NAM	name (residence or office occupant)	alphanumeric
PC/ZIP	postal/ZIP code	alphanumeric

[3] RD should be used in preference to A6. A6 must be accepted by the ECRF

BLD	building (structure)	alphanumeric
UNIT	unit (apartment, suite)	alphanumeric
FLR	floor	alphanumeric
ROOM	room	alphanumeric
PLC	type of place	alphanumeric
PCN	postal community name	alphanumeric
POBOX	post office box (P.O. box)	numeric
ADDCODE	additional code	alphanumeric
SEAT	Seat (desk, workstation, cubicle)	alphanumeric
RD	primary road name	alphanumeric
RDSEC	road section	alphanumeric
RDBR	branch road name	alphanumeric
RDSUBBR	sub-branch road name	alphanumeric

PRM	Road name pre-modifier	alphanumeric
POM	Road name post-modifier	alphanumeric

No individual element in a civic address stored in the ECRF shall be longer than 256 bytes.

To provide this data, the ECRF uses layer replication of one or more SIFs that cover the ECRF's service area. The source SIF may be provided by 112 authorities, or other government agencies with GIS responsibility (e.g., a county mapping agency and/or responders who define their own service areas). The ECRF mapping data is provided by:

Table 4-4. Civic Location Data Elements

PIDF Element	**Layer Name**	**Geometry or Attribute**
country	None, provisioned	None
A1	State	Name
A2	County	Name
A3	Municipality	Name
A4	City Division	Name
A5	Neighborhood	Name
A6	Street Centerline or Street Geometry	Name
PRD	Same as A6	PRD
POD	Same as A6	POD
STS	Same as A6	STS
HNO	Address Point or Parcel or sub parcel	HNO
HNS	Same as HNO	HNS

LMK	Same as HNO	LMK
LOC	Same as HNO	LOC
NAM	Same as HNO	NAM
PC/ZIP	ZIP code	Name
PCN	ZIP code	Post Office
RD	Same as A6	Name
PRM	Same as A6	PRM
POM	Same as A6	POM

4.4.3.2 Service Boundaries

Location represented by geodetic coordinates provides data that corresponds to a specific geographic location point. It is possible to represent a larger geographic area, such as a PSAP serving area as a polygon set. More than one polygon may occur in the set when the service area has holes or non-contiguous regions.

For each service urn supported by an ECRF, one or more layers will provide polygon sets associated with URIs. Two attributes are used on these polygons:

URN: The service URN this boundary is associated with

URI: The URI returned if the location is within the boundary

The ECRF 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.

4.4.3.3 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 determines which URI is returned. Therefore, it will be necessary to be able to associate multiple URIs with a service boundary. URI format is described in IETF RFC 3986, *Uniform Resource Identifier (URI): Generic Syntax*. 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 K, which is the maximum size of a packet on the ESInet, less any header information.

4.4.3.4 Other Data

- ECRF Identifier - contains a LoST application unique string identifying the authoritative generator of the mapping
- ECRF mapping identifier - identifies a particular mapping and contains an opaque token that must be unique among all different mappings maintained

by the authoritative source for that particular service. For example, a Universally Unique Identifier (UUID) is a suitable format.

- Date and time mapping was last updated – contains the XML data type dateTime in its timezoned form, using canonical UTC representation with the letter 'Z' as the time zone indicator.
- Date and time of mapping expiration – contains a timezoned XML type dateTime, in canonical representation. Optionally, this attribute may contain the values of 'NO-CACHE' and 'NO-EXPIRATION' instead of a dateTime value. The value 'NO-CACHE' is an indication that the mapping should not be cached. The value of 'NO-EXPIRATION' is an indication that the mapping does not expire.
- Display name – contains a description of the service using a string that is suitable for display to human users, which may be annotated with the 'xml:lang' attribute that contains a language tag to aid in the rendering of text. The display name is used as the "English Language Translation" (ELT) and must be provided for all responder URIs.
- Service identifier for which mapping is valid
- Service boundary definition – Service boundaries must be defined using exactly one of the two baseline profiles (i.e., geodetic-2d, civic), in addition to zero or more additional profiles. A location profile MUST define:
  - The token identifying it in the LoST location profile registry;
  - The formal definition of the XML to be used in requests, i.e., an enumeration and definition of the XML child elements of the <location> element;
  - The formal definition of the XML to be used in responses, i.e., an enumeration and definition of the XML child elements of the <serviceBoundary> element;
  - The declaration of whether geodetic-2d or civic is to be used as the baseline profile. It is necessary to explicitly declare the baseline profile as future profiles may be combinations of geodetic and civic location information.

To support the delivery of service boundary information using the geodetic 2d profile in a response to a client, the ECRF must support the following location shapes:

- Point
- Polygon
- Circle
- Ellipse
- Arcband

To support civic service boundaries, each service boundary consists of the set of civic addresses that fall within the service boundary, namely all the addresses that textually match the civic address elements provided, regardless of the value of the other address elements. A location falls within the mapping's service boundary if it matches any of the service boundary elements.

Note that the provisioning interface to the ECRF is the SIF layer replication protocol, and thus always delivers a geodetic service boundary definition to the ECRF. The ECRF 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.

- Service boundary reference definition - The identifier must be globally unique. It uniquely references a particular boundary. It could be a locally unique token and the hostname of the source of the boundary separated by an '@'
- Service number - contains a string of digits, * and # that a user on a device with a 12-key dial pad could use to reach that particular service.

4.4.4 Recursive and Iterative Query Resolution

An ECRF may receive a query for a location that is not within its internal database. For such queries, it may redirect the querier to another ECRF (iteration), or it may query the other ECRF and return the result to the querier (recursion). Which action it takes is primarily determined by a query parameter, but may be limited by provisioning and may depend on the location in the query. For example, it may allow recursive resolution for any in-state queries but insist on redirecting an out-of state query to the national forest guide, see Section 4.14.

Each country should have one or more ECRF(s) and/or forest guide which can resolve, by iteration or recursion, any query. The country-level ECRF should have boundaries for every authoritative ECRF in the state as well as the ability to redirect out of country queries to the respective forest guides. It may have knowledge of adjacent state ECRFs. Any lower level ECRF can refer or redirect any query it cannot handle to its state ECRF, which can refer or redirect to another ECRF in the state or can consult the national forest guide. It is recommended that ECRFs handle queries via recursion.

All ECRFs must provide the proper <path> element as described in RFC5222.

4.4.5 Coalescing Data and Gap/Overlap Processing

ECRFs may coalesce data from several 112 Authorities. The resulting database appears to be a seamless route database for the union of the service areas of each 112 authority. Such ECRFs are provisioned to accept data from multiple SIFs.

In some local SIFs, for convenience, some area beyond the service boundary of the PSAPs the 112 Authority provides data for may be present. If so, this area must be marked with an "Informative" attribute, and the ECRF will ignore it.

When the data is coalesced, boundaries may have gaps and overlaps. The relevant 112 Authorities should endeavor to address such issues early, but despite best efforts, the ECRF may encounter a gap or overlap. The ECRF must have a provisionable threshold parameter that indicates the maximum gap/overlap that is ignored by the ECRF. This threshold is expressed in square meters. Gaps or overlaps that are smaller that this parameter must be handled by the ECRF 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 source SIFs.

The ECRF must report gaps and overlaps larger than the provisioned threshold. To do so, it makes uses of the GapOverlap event. All 112 Authorities who provide source GIS data to an ECRF must subscribe to its GapOverlap event. The event notifies both agencies when it receives data that shows 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 response of the agencies must be updates to the data that address the gap/overlap. The ECRF will repeat the notification at least daily until it is resolved (by changing the SIF 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 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 source SIFs.

The GapOverlap event is defined as follows:

Event Package Name: EES-GapOverlap

Event Package Parameters: none

SUBSCRIBE Bodies: standard RFC4661 + extensions filter specification may be present

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

NOTIFY Bodies: MIME type application/vnd,EES.GapOverlap+xml

Parameter	Condition	Description
Agency	Mandatory	URI of Agency with gap/overlap. Will be repeated at least twice
Layer	Mandatory	Enumeration of layer where gap/overlap exists.

		May occur multiple times
Gap	Mandatory	Boolean, True if gap, false if overlap
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.

4.4.6 Replicas

An ECRF is essentially a replica of a subset of the layers of one or more SIFs. The ECRF in turn, may provide a feed to other ECRFs who wish to maintain a copy of the data in an ECRF. As the ECRF is not the data owner, the source SIF must have a policy that permits the ECRF to do so, and the policy may restrict which entities the ECRF may provide replication data to. The ECRF also has a policy that defines who it will provide data to. If the ECRF provides a replica service, the interface is the layer replication service. In this case, the ECRF is the server side, as opposed to the client interface it must provide towards the SIF(s) it receives data from.

4.4.7 Provisioning

The ECRF is provisioned with

- a set of layers from one or more SIFs.
- 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 should be provisioned with every sos urn in the IANA registry[4]. All sos service URNs that represent services provided by the PSAP return the dial string '112' and the PSAP URI. Other services available in the area would typically return a tel uri with the proper PSTN telephone number.

4.4.8 Roles and Responsibilities

The ECRF plays a critical role in the location-based routing of emergency calls. Therefore, it is crucial that the data in the ECRF be accurate and authorized. EENA therefore expects that 112 Authorities will be responsible for inputting the authoritative data for their jurisdiction in the ECRF. The data may be aggregated at a regional or state level, and the ECRF system provided at that level may be the responsibility of the associated state or regional emergency communications agency. In addition, access or calling network operators may maintain replicas of the ECRF. Thus the operation and maintenance of individual ECRFs may be the responsibility of the provider of the network in which they physically reside, but it is the 112 Authority that is responsible for maintaining the integrity of the source data housed within those systems. The 112 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.

4.4.9 Operational Considerations

The NG112 architecture allows for a hierarchy of ESInets, with replicas of ECRFs 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 112 Authority's ECRF must be accessible from the Internet[5]. 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

[4] While there is only one common emergency service number, 112, in Europe, 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.

[5] The Internet accessible ECRF may be a state or regional ECRF containing the local ECRF data of all 112 Authorities within the state or region

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. Provisioning of data within appropriate ECRF systems for use in overload and backup routing scenarios must also be supported.

4.5 Location Validation Function

The NG112 solution must properly route incoming IP packet-based emergency calls to the appropriate PSAP, as well as support the dispatch of responders to the right location. The location information used, when provided in civic form, must be proved sufficient for routing and dispatch prior to the call being placed. We refer to this as having a "valid" location for the call[6]. This architecture defines a function called the LVF (Location Validation Function) for this purpose. The LVF is generally only used for civic location validation. Geo coordinate validation has some limited use, in extreme cases, including national boundary routing scenarios, over coastal waters, etc. 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][7]. For fixed endpoints, location must be validated when the device is deployed, at each boot-up (power-cycle), and periodically, in order to reach the level of assurance required for acceptable route quality. For Nomadic devices, an LVF request must be invoked as in the fixed case, and in addition, whenever an end device changes its location. Mobile location differs in that it is expected to use only geo-coordinates (e.g., lat/lon), and therefore does not require the same level of LVF interaction and may not require any LVF interaction.

4.5.1 Functional Description

The Location Validation Function (LVF) should be engineered to respond to LVF clients within a few seconds. The LVF data and interfaces are similar to those used by an ECRF representing the same geographic area(s). As a result, the LVF shares

[6] 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. NG112 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.

[7] Short periods (days or a few weeks) allow errors that arise due to changes in underyling 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 period of 30 days is recommended. LIS operators may wish to consult with the LVF operator to determine an optimal revalidation period.

the same SIF data layer information as the ECRF, and reuses the same LoST protocol that is used by the ECRF, yet with a few additional data elements. The LVF supports an input query mechanism requiring civic location, a service URN, and a validation flag. This validation flag is an xml parameter setting, and is the main difference between a LoST query intended for an LVF and a LoST query used for routing, that is issued to an ECRF.

Messaging that is returned from an LVF contains all the same data as is returned from an ECRF query. In addition, an LVF validation query response also includes an indication of which data elements were found within the LVF itself. It's this address field matched data that enables the LVF client to determine if the civic location provided in the input is considered valid, and to what level of granularity.

Many other aspects of the LVF, its interfaces, and the data it contains are identical to the ECRF. Please refer to those sections for more detail.

4.5.2 Interface Description

The LVF supports two interfaces: a query/response interface, and a provisioning interface. Since the LVF is based on the LoST server architecture, the validation query/response interface is defined as the LoST protocol, per RFC5222 [61].

RFC5222 section 8.4.2 states that the inclusion of location validation is optional, and subject to local policy. LTD NG112 architecture requires that all LoST server implementations, deployed as an LVF, must support the inclusion of location validation information in the "findServiceResponse" message.

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 over 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.

LVF interaction at emergency call time may be performed by a PSAP.

4.5.2.1 User Endpoint interaction

Any user endpoint (i.e., UE, device, handset, client application, etc.) that will perform a location validation directly, must implement the LVF (LoST) interface to be able to access an LVF. The endpoint must use the LVF interface with the same service URN as would be used for a routing query to the ECRF, viz "urn:service:sos", along with location information.

4.5.2.2 LIS Interaction

The LVF may receive a location validation request from the LIS in order to assure that the location information along with a particular service URN, used in the LVF query, will be deemed "valid", that is, that there exists an appropriate route URI (e.g., PSAP URI) to match the query. The LVF must return the same URI that the ECRF would have returned (and subsequently will return at emergency call time), based on the same inputs used for the LVF.

4.5.2.3 Provisioning Interaction

The LVF requires the same type of data as required with the ECRF, and is expected to be provisioned through an xml provisioning interface either manually or via a machine-to-machine implementation. This includes synchronization between redundant and tiered LVF elements.

4.5.3 Interface Description

Currently, the LVF supports several interfaces, including the following:

- validation query interface
- validation response interface
- provisioning interface
- time interface
- logging interface
- SIF layer replication protocol.

4.5.3.1 Validation query interface:

Examples taken from Figures 5 & 6 of RFC 5222.

Example of a validation request message:

```
<?xml version="1.0" encoding="UTF-8"?>
<findService
  xmlns="urn:ietf:params:xml:ns:lost1"
  recursive="true"
  validateLocation="true"
  serviceBoundary="value">
  <location id="627b8bf819d0bad4d" profile="civic">
    <civicAddress
      xmlns="urn:ietf:params:xml:ns:pidf:geopriv10:civicAddr">
      <country>US</country>
      <A1>OH</A1>
      <A3>Middletown</A3>
      <RD>Main</RD>
      <STS>ST</STS>
```

```
   <HNO>123</HNO>
   <PC>45054</PC>
  </civicAddress>
 </location>
 <service>urn:service:sos </service>
</findService>
```

4.5.3.2 Validation response interface

The LVF, for validation, only supports the “findServiceResponse” message. In the following example of a validation response message, note the bolded elements that indicate the validation:

```
<?xml version="1.0" encoding="UTF-8"?>
<findServiceResponse xmlns="urn:ietf:params:xml:ns:lost1">
 <mapping
  expires="2010-01-01T01:44:33Z"
  lastUpdated="2009-11-01T01:00:00Z"
  source="authoritative.example"
  sourceId="4db898df52b84edfa9b6445ea8a0328e">
  <displayName xml:lang="en">
   Middleton PSAP
  </displayName>
  <service>urn:service:sos</service>
  <serviceBoundary profile="civic">
   <civicAddress
    xmlns="urn:ietf:params:xml:ns:pidf:geopriv10:civicAddr">
    <country>US</country>
    <A1>Ohio</A1>
    <A3>Middelton</A3>
    <PC>45054</PC>
```

```
      </civicAddress>
    </serviceBoundary>
    <uri>sip:middleton-psap@example.com</uri>
    <uri>xmpp:middleton-psap@example.com</uri>
    <serviceNumber>911</serviceNumber>
  </mapping>
  <locationValidation>
    <valid>country A1 A3 A6 STS</valid>
    <invalid>PC</invalid>
    <unchecked>HNO</unchecked>
  </locationValidation>
  <path>
    <via source="resolver.example"/>
    <via source="authoritative.example"/>
  </path>
  <locationUsed id="627b8bf819d0bad4d"/>
</findServiceResponse>
```

The basis of a validation response is the inclusion of the data element, "validateLocation" being set to "true" in the validation query. In addition to the regular default inputs being returned, the validateLocation=true attribute setting will result in a response using the xml element "findServiceResponse" containing sub-element "locationValidation", with attributes and tokens relating to which input elements were checked and shown as valid (or invalid).

The ECRF supports the <locationValidationUnavailable> warning element when an LVF server seeks to notify a client that it cannot fulfill a location validation request. This warning allows a server to return mapping information while signaling this exception state, see Section 13.3 of [RFC5222].

4.5.3.3 LVF Provisioning/synchronization

The LVF provisioning interface the same as that of the ECRF and uses the SIF Layer Replication protocol

4.5.3.4 Alternative Address Interface

The ability to have alternative addresses returned is currently out-of-scope for this document, and is left for future consideration.

4.5.3.5 Time Interface

The LVF must implement an NTP client interface in order to maintain current, accurate time-of-day information. The time of day information is an input to the LVF validation response information, as well as each transaction to the logging interface.

4.5.3.6 Logging Interface

The LVF must implement a logging interface per Section 4.13.1.1. The LVF must be capable of logging every incoming validation request along with every recursive request and all response messages. In addition, the LVF must log all provisioning and synchronization messages and actions. In addition to the requirement for logging all the same data elements currently defined for logging by the ECRF, we have additional specific data logging requirements.

4.5.3.6.1Validation query logging

The LVF logging mechanism must be capable of logging all input data elements for a validation query, including the specific input location and service URN. All logging transactions must be stored in the form of transaction detail records, and must be made external when warranted by implementation policy. The data elements logged include the following:

- Date & Time of transaction
- Request message type
- Type of location received
- Location elements received
- Service URN received.

4.5.3.6.2Validation response logging

The LVF logging mechanism must be capable of logging all output data elements provided in the validation response message, including the validation response status of each location element. All logging transactions must be stored in the form of transaction detail records, and must be made external when warranted by implementation policy. The data elements logged include the following:

- Date & Time of transaction
- Response message type
- Validation attributes
- Location element tokens
- "Error Code" values.

4.5.3.6.3Provisioning/Synchronization logging

The LVF logging mechanism must be capable of logging all provisioning input and output messages from an individual provisioning client or another LVF. All logging transactions must be stored in the form of transaction detail records, and must be made external when warranted by implementation policy. The data elements logged include the following:

- Date & Time of transaction
- Transaction type (e.g., Add, Delete, Modify)
- Record information
- Response acknowledgement.

4.5.4 Data Structures

The data structures for the LVF include those defined for the ECRF. In addition to those used for the ECRF, the following LVF specific data structures are included:

Table 4-1 LVF Specific Location Data Elements

Label	Description	Type	Example
validateLocation	Xml attribute for findService elementvalidation (see notes 1 & 2)	Boolean	true
locationValidation	Xml attribute for findServiceResponse element	n/a (see note 3)	n/a
valid	Xml attribute to list those input element tokens that were successfully validated	n/a (see note 3)	A1
invalid	xml attribute to list those input element tokens that were unsuccessfully validated	n/a (see note 3)	RD
unchecked	Xml attribute to list those input element tokens that were not checked for validation (see note 3)	n/a (see notes 3 & 4)	HNO

Note 1. *If the validateLocation is not included, it is treated as "false".*

Note 2. *The attribute is ignored if the input contains a geodetic form of location.*

Note 3. RFC5222 states only that the presence of each element token is optional, subject to local policy.

Note 4. Any input element tokens not included in the locationValidation response, belong to the "unchecked" category.

4.5.5 Roles and Responsibilities

112 Authorities are directly responsible for LVF data, though a PSAP may contract data maintenance over to a third-party if they choose to. The LVF provisioning interface is the SIF layer replication protocol.

The ECRF and the LVF are provisioned, directly or indirectly, from an authoritative SIF, using the layer replication protocol. A change in the SIF will be propagated to any ECRFs and LVFs connected to that SIF system. Thus the ECRF and LVF do not have to be provided by, or operated by the same entity, although it will be common for them to be so connected. Indeed, it may be common for the ECRF and LVF to be collocated in the same box.

4.5.6 Operational Considerations

The placement of 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 NG112 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. Finally, 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[8].

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 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.

[8] The Internet accessible LVF may be a state or regional LVF containing the local LVF data of all PSAPs within the state or region

An LVF, wherever deployed, whether within an Access network, or in some other type of Origination network, needs to be able to reach out to other LVFs in case of missing data, or in the case where the requested location is outside its local jurisdiction. If the LVF doesn't know the answer, based on configuration, it will either recurse (refer) a request for validation to one or more other LVFs, or it will iterate the request to some other LVF, providing the other LVF's URL in the original LVF response.

Redundant LVF elements are recommended, similar to DNS server deployments (the LVF shares some of the same replication characteristics with DNS), by example, in order to maintain a high level of availability and transaction performance.

As with the ECRF, and given the close association between the LVF and ECRF elements, 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 LVF. This level of redundancy aids in maintaining high levels of availability during unexpected system outages, scheduled maintenance windows, data backup intervals, etc.

Similar to ECRF deployments, localized LVF elements may have limited data, sufficient to provide location validation within its defined boundaries, but must rely on other LVFs for validation of a location outside its local area.

LVFs within the ESInet will likely have considerably more data than those LVFs in origination networks, providing aggregation for many local access areas as well as PSAP jurisdictions. Even the level of data that an 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 LVF, only base civic location data for its described jurisdiction, whereas a State-level or County-level LVF may aggregate all of the local PSAP data within that level of hierarchy.

4.6 Spatial Information Function

The Spatial Information Function (SIF) is the base database for NG112. Nearly all location related data is ultimately derived from the SIF. If a datum is somehow associated with location, the base data will reside in the SIF. The SIF supplies data for:

1. The ECRF/LVF
2. Map views for alternate PSAPs.

The SIF is a specialized form of a Geospatial Information System, and may be implemented on a conventional GIS with the appropriate interfaces. The SIF itself is not standardized in this architecture. What is standardized is a method of replicating layers from the master SIF to external databases. The ECRF and LVF provisioning interfaces use this mechanism. When calls are answered at an alternate PSAP, map views are generated from off-site replicas of layers in the SIF system, which are maintained by this interface.

4.6.1 Layers

In order to be useful, this document standardizes certain layers in the SIF system so that interchange between SIF systems is practical. The NG112 system is dependent on all SIF systems having common definitions for these layers. All attributes will be listed in further versions of this document. The layers to be defined include:

- Layers with polygon features
    - State (PIDF A1)
    - County (PIDF A2)
    - Municipality (PIDF A3)
    - Division (PIDF A4)
    - Sub-Division (PIDF A5)
    - Parcels (Can be PIDF HNO and components)
    - Sub-Parcels (Can be PIDF HNO and components)
    - PSAP Service Boundary
    - Responding Agency Services Boundary – Law Enforcement, EMS, Fire, Highway Patrol, etc…
- Layers with line features
    - Road Centerlines (PIDF RD and components)
- Layers with point features
    - Site / Structure Locations (address points) (PIDF HNO and components)

4.6.2 Geocode Service (GCS)

The Geocode service provides geocoding and reverse geocoding. Two functions are defined:

Geocode: which takes a PIDF-LO as described in RFC4119 updated by RFC5139 and RFC5491 containing a civic address and returns a PIDF-LO containing a geo for the same location.

ReverseGeocode: which takes a PIDF-LO as described in RFC4119 updated by RFC5139 and RFC5491 containing a geo and returns a PIDF-LO containing 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 SIF. 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 SIF has 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 GCS uses a forest guide referral mechanism identical to the ECRF. If the input address is not within the service boundary of the local GCS, it can consult a forest guide to refer the query to the appropriate GCS.

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.

GeocodeRequest

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

GeocodeResponse

Parameter	**Condition**	**Description**
pidflo	Conditional	PIDF-LO resulting from conversion
referral	Conditional	URI of another GCS
errorCode	Mandatory	Error response, see below

Either pidf or referral must be present in the response

Error Codes

100 Okay No error

508 NoAddressFound: the input appears to be within the service boundary of the GCS, but no point matching the input was located

509 Unknown MCS: 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	PIDF-LO resulting from conversion
referral	Conditional	URI of another GCS
errorCode	Mandatory	Error response, see below

Either pidflo or referral must be present in the response

Error Codes

100	Okay No error
508	NoAddressFound: the input appears to be within the service boundary of the GCS, but no point matching the input was located
509	Unknown MCS: 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.

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 interface in a future edition of this document.

4.6.3 Operational Considerations

The SIF is not used directly in call processing, although its data is critical to achieving proper routing. For that reason, a single SIF system, with frequent backup operations is sufficient. However, since calls may be answered by other PSAPs, and the originally intended PSAP may be unavailable, copies of the layers sufficient for display should be made available, using the layer replication mechanism.

4.7 PSAP

A PSAP provides the following interfaces towards the ESInet:

4.7.1 SIP Call interface

The PSAP must deploy the SIP call interface as defined in Section 5.1 including the multimedia capability, and the non-human-associated call (emergency event) capability. PSAPs must recognize calls to their administrative numbers received from the ESInet (and distinguishable from normal 112 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 Route header). The SIP call interface may also be used to place calls (including callbacks) from the PSAP using normal SIP trunking mechanisms, as specified in sipConnect V1.0 [108].

Note: *There is no mechanism by which a caller could discover what media the PSAP supports beyond the basic SIP call setup negotiation mechanism. This will be covered in a future edition of this document.*

4.7.2 LoST interface

The PSAP must provide a LoST client interface as defined in Section 5.5. 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 ECRF and LVF use the LoST interface.

4.7.3 LIS Interfaces

The PSAP must implement both SIP Presence Event Package and HELD dereference interfaces to any LIS function as described in Section 4.10. When the PSAP receives a location reference (in a Geolocation header on the upstream SIP interface) it uses the LIS dereference interface to obtain a location value. The PSAP must be provisioned with credentials for every LIS in its service area[9]. The PSAP must use TCP with either TLS or IPsec for the LIS Dereference 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 will result in a location meeting regulated 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.

[9] 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 LIS’s that do not accept the PCA credential.

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 in loc-filters [103] and rate-control [113] 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, if available in an E112, ALI has no equivalence in NG112.

4.7.4 Bridge Interface

A PSAP may deploy a bridge (as described in Section 4.8) 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.

4.7.5 ElementState

The PSAP must deploy an ElementState notifier as described in Section 5.6.2. Note that the terminating ESRP may route to a (queue of) call taker(s). Each call taker should implement an element state notifier.

4.7.6 SIF

The PSAP may provide 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).

4.7.7 Logging Service

The PSAP may deploy a logging service (as described in Section 4.13) inside the PSAP, in which case it must provide the logging service retrieval functions. A PSAP may use a logging service in the ESInet, in which case it must deploy the logging service insert functions.

4.7.8 Security Posture

The PSAP must provide a Security Posture notifier as described in Section 5.6.1.

4.7.9 Policy

The PSAP may provide a policy store as described in Section 5.4.1, 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 for the queue(s) its calls are sent to.

PSAPs must provide a takeCallsOnQueues policy to determine which queues the PSAP will dequeue from (that is, which queues it will subscribe to the dequeueRegistration and queueState events for).

4.7.10 Additional Data dereference

The PSAP must deploy a dereference (HTTP Get) interface for additional data as described in Section 8.

4.7.11 Time Interface

The PSAP must implement an NTP client interface for time-of-day information. The PSAP may also provide an interface to a hardware clock.

4.7.12 Test Call

The PSAP may deploy the test call function as described in Section 12.

4.7.13 Call Diversion

A PSAP may be overloaded and be unable to answer every call 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 Multimedia Response unit
- Calls can be diverted to one or more alternate PSAPs.

The latter is mechanized by sending the call to queues, which other PSAPS dequeue from. Since the diverted-to PSAP(s) have to explicitly register to dequeue (DequeueRegistration, see Section 4.3.1.2), 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 subscribes to the DequeueRegistration event of the diverted-from PSAP with the "Standby" parameter set to "true". The diverted-to PSAP also subscribes to the queueState event for the diversion queue. 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 resubscribe to the DequeueRegistration event with Standby set 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>true</standby>.

4.7.14 Incidents

A new call arrives with a new Incident Tracking Identifier assigned by the first ESRP in the ESInet. The ESRP assumes each 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. The actual IncidentTrackingID would be part of the AdditionalPSAPData 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.

4.8 Bridging

Bridging is used in NG112 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 (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 following table provides an overview of the different bridging concepts described in this document and illustrates the pros and cons as well as implementation recommendations.

Section in LTD doc		Topic	Referenced Specification	Note	Pros	Cons
4.8.1		Conference Using SIP Ad-Hoc Methods	RFC 4579	Replaces header support (by caller or components in the path)	Standard mechanism when end devices support RFC 4579.	Creates problems when end devices do not support the REFER mechanism.
4.9		Transfer Involving Calling Devices that Do Not Support Replaces	RFC3261	Devices that could originate 112 calls do not support the Replaces header	-	-
Option #1	4.9.1	B2BUA	RFC 3261	Introduce a B2BUA function which terminates the REFER	BCFs should support option #1; One transfer mechanism for PSAPs. B2BUA can separate between signaling and media	Emergency calls that go to wrong location end up being anchored in a B2BUA in the original location. →REFER/REPLACES methods suggested, but can do local transfer if the far-end doesn't support REFER/ Replaces
Option #2	4.9.2	Bridging at the PSAP Using Third Party Call Control in the Call Taker User Agent	RFC 3725	The initial answering UAC becomes a signaling B2BUA; call taker UA receiving a call which does not contain a Supported header indicating support for Replaces	PSAP CPE may support option #2, which has no impact or dependency on other elements	This option is similar to option 1 but instead of using a B2BUA at a decided entity (like an SBC) the answering UAC acts as an B2BUA

Option #3	4.9.3	Answer all calls at a bridge	Non-standard	All incoming 112 calls are answered at a bridge	PSAP CPE may support option #3 if the bridge support is available. Voice Recording is easier.	No standard off-the-shelf bridges available to handle call continuity; PSAP has to be aware of the transfer. Emergency calls that go to wrong location end up being anchored in a bridge in the original location.

4.8.1 Bridge Call Flow

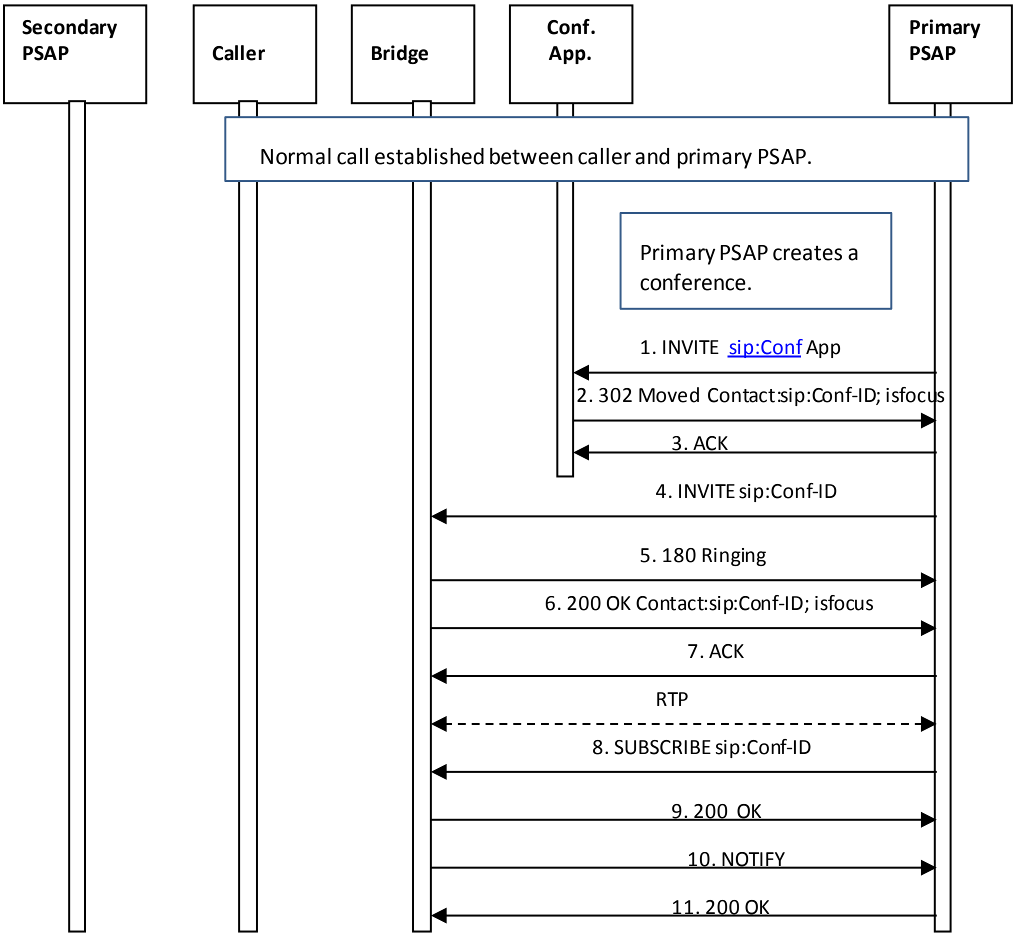
Conferencing procedures are documented in RFC 4579. The high-level protocol sequence as defined in RFC 4579 [51] is as follows:

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.

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 4.9

4.8.1.1 Creation of a Conference Using SIP Ad-Hoc Methods

This scenario described in the call flow depicted below follows Section 5.4 of RFC4579.



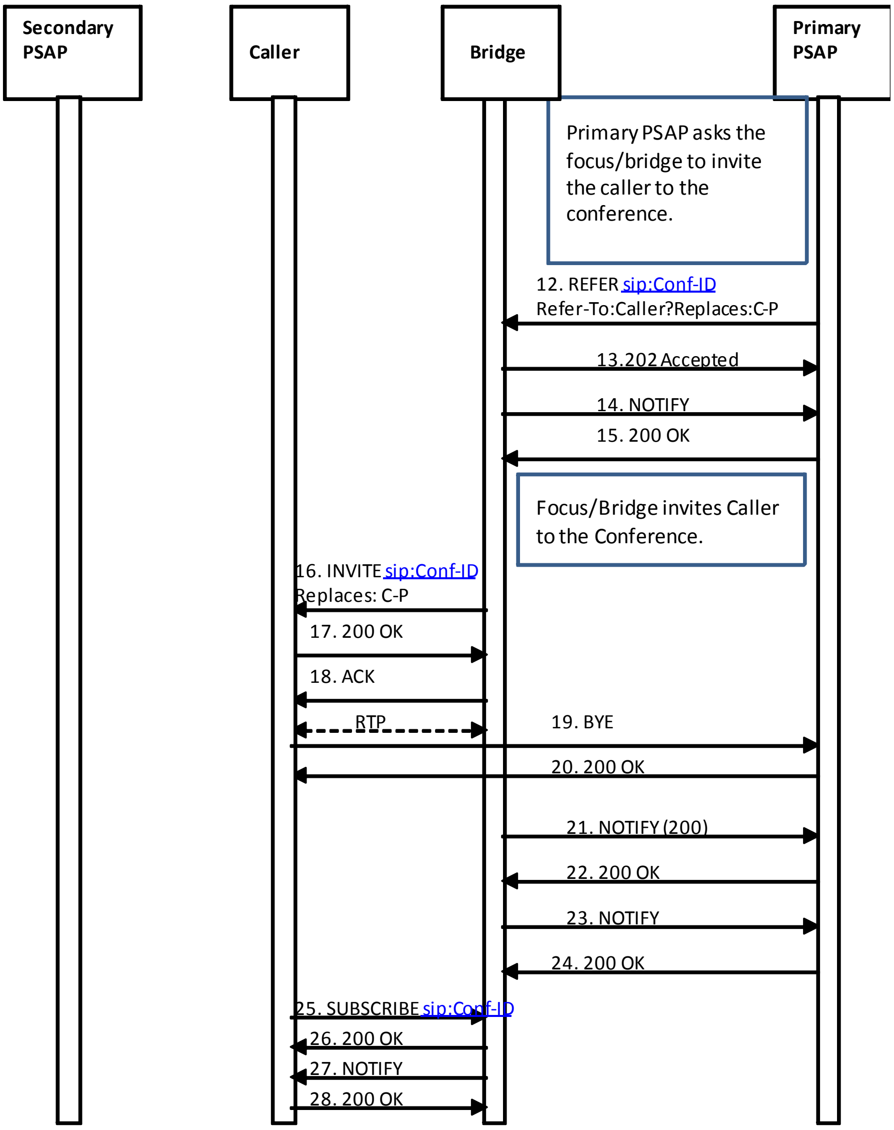
1. The Primary PSAP creates a conference by first sending an INVITE to a conference application, using a URI that is known by/provisioned at the Primary PSAP.
2. The Conference Application responds by sending a 302 Moved message, which redirects the Primary PSAP to the conference bridge, and provides 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.[10]
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.

4.8.1.2 Primary PSAP Asks Bridge to Invite the Caller to the Conference

This flow is based on Section 5.10 of RFC 4579.

[10] 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.



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.

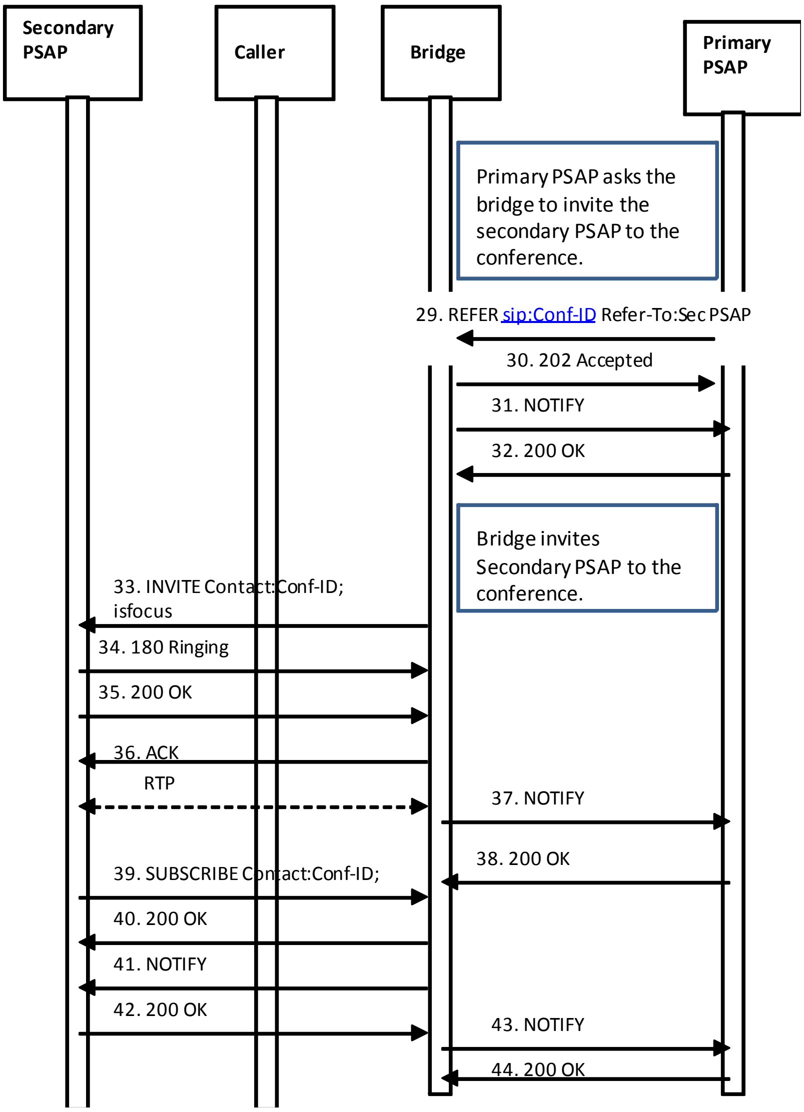
16. The bridge invites the caller to the conference by sending an INVITE method containing the Conf-ID and a Replaces header that references the leg between the caller and the Primary PSAP.
17. The caller accepts the invitation by returning a 200 OK message.
18. The bridge acknowledges receipt of the 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)

4.8.1.3 Secondary PSAP is Invited to the Conference

This flow is based on Section 5.5 of RFC4579.


Secondary PSAP
Caller
Bridge
Primary PSAP
Primary PSAP asks the bridge to invite the secondary PSAP to the conference.
29. REFER sip:Conf-ID Refer-To:Sec PSAP
30. 202 Accepted
31. NOTIFY
32. 200 OK
Bridge invites Secondary PSAP to the conference.
33. INVITE Contact:Conf-ID; isfocus
34. 180 Ringing
35. 200 OK
36. ACK
RTP
37. NOTIFY
38. 200 OK
39. SUBSCRIBE Contact:Conf-ID;
40. 200 OK
41. NOTIFY
42. 200 OK
43. NOTIFY
44. 200 OK

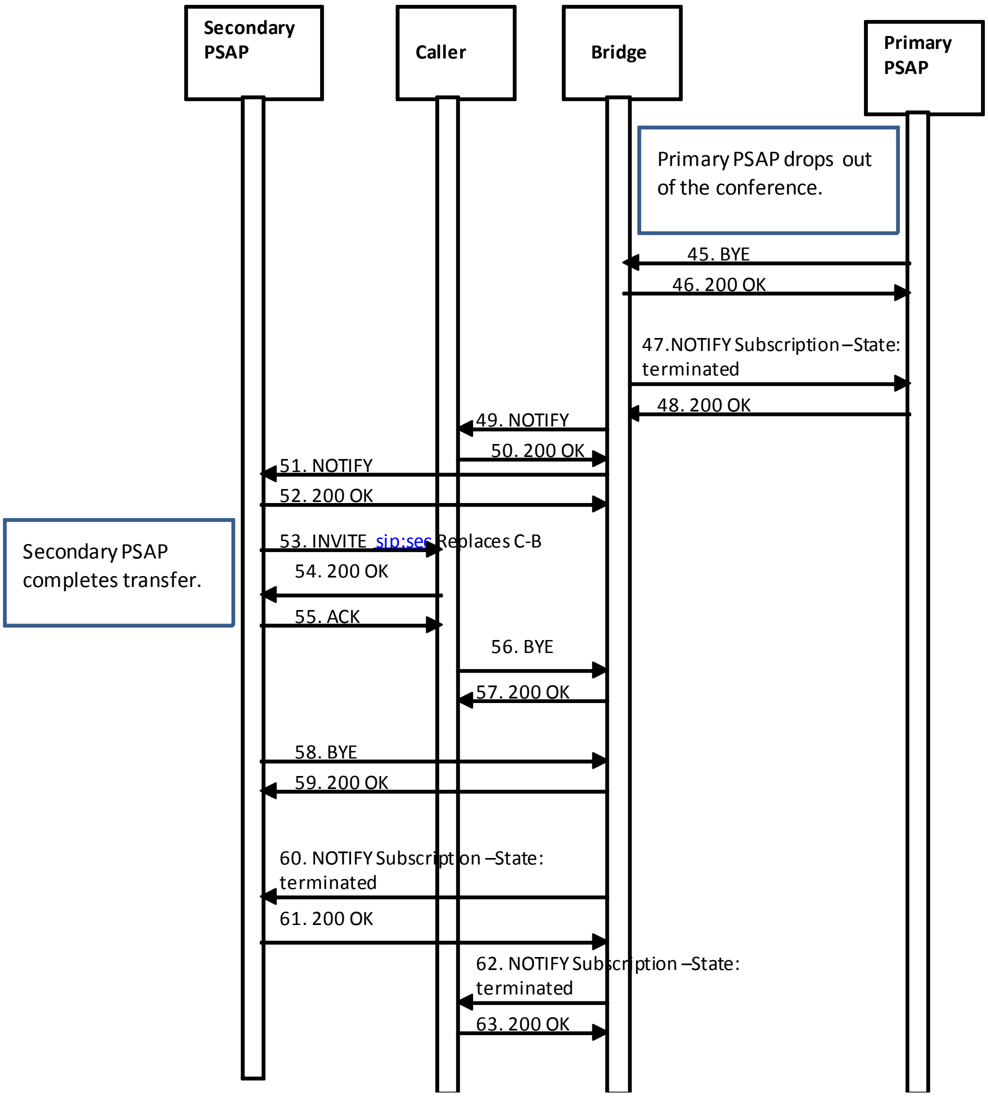
29. The Primary PSAP sends a REFER method to the conference bridge asking it to invite the Secondary PSAP to the conference. The REFER method contains the Conf-ID and a Refer-To header that contains the URI of the Secondary PSAP. The REFER method also contains an escaped Call-Info header field containing a reference URI that points to the "Additional Data Associated with a PSAP" data structure.
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 "Additional Data Associated with a PSAP" data structure.
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.

4.8.1.4 Primary PSAP Drops Out of Conference; Secondary PSAP Completes Transfer


Secondary PSAP
Caller
Bridge
Primary PSAP
Primary PSAP drops out of the conference.
45. BYE
46. 200 OK
47.NOTIFY Subscription –State: terminated
48. 200 OK
49. NOTIFY
50. 200 OK
51. NOTIFY
52. 200 OK
Secondary PSAP completes transfer.
53. INVITE sip:sec Replaces C-B
54. 200 OK
55. ACK
56. BYE
57. 200 OK
58. BYE
59. 200 OK
60. NOTIFY Subscription –State: terminated
61. 200 OK
62. NOTIFY Subscription –State: terminated
63. 200 OK

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 "Additional Data Associated with a PSAP" data structure
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.

4.8.2 Passing data to Agencies via bridging

When another PSAP is bridged to a 112 call there are separate "legs" for each participant in the bridge. The 112 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 a conference. It is critical that the transfer target receive (or have access to) the location of the original caller, as well as any "Additional Data" that the primary PSAP call taker may have accessed or generated during the processing of the emergency call. Caller location information received by the primary PSAP in the Geolocation header of the INVITE message, along with any additional data that the primary PSAP call taker may have obtained when the call was delivered (i.e., "Additional Data Associated with a Call" and/or "Additional Data Associated with a Caller") or that was generated by the call taker as a result of processing the incoming emergency call, should be populated in the "Additional Data Associated with a PSAP" structure. (See Section 8 for further discussion of Additional Data structures.) When an emergency call is transferred, the primary PSAP will request that the bridge insert by embedded header, a Call-Info header with a URI that points to the "Additional Data Associated with a PSAP" data structure in the REFER method sent to the bridge. The bridge must subsequently include this Call-Info header in the INVITE it sends to the transfer target.

4.9 Transfer Involving Calling Devices that Do Not Support Replaces

There is a problem that some devices that could originate 112 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.

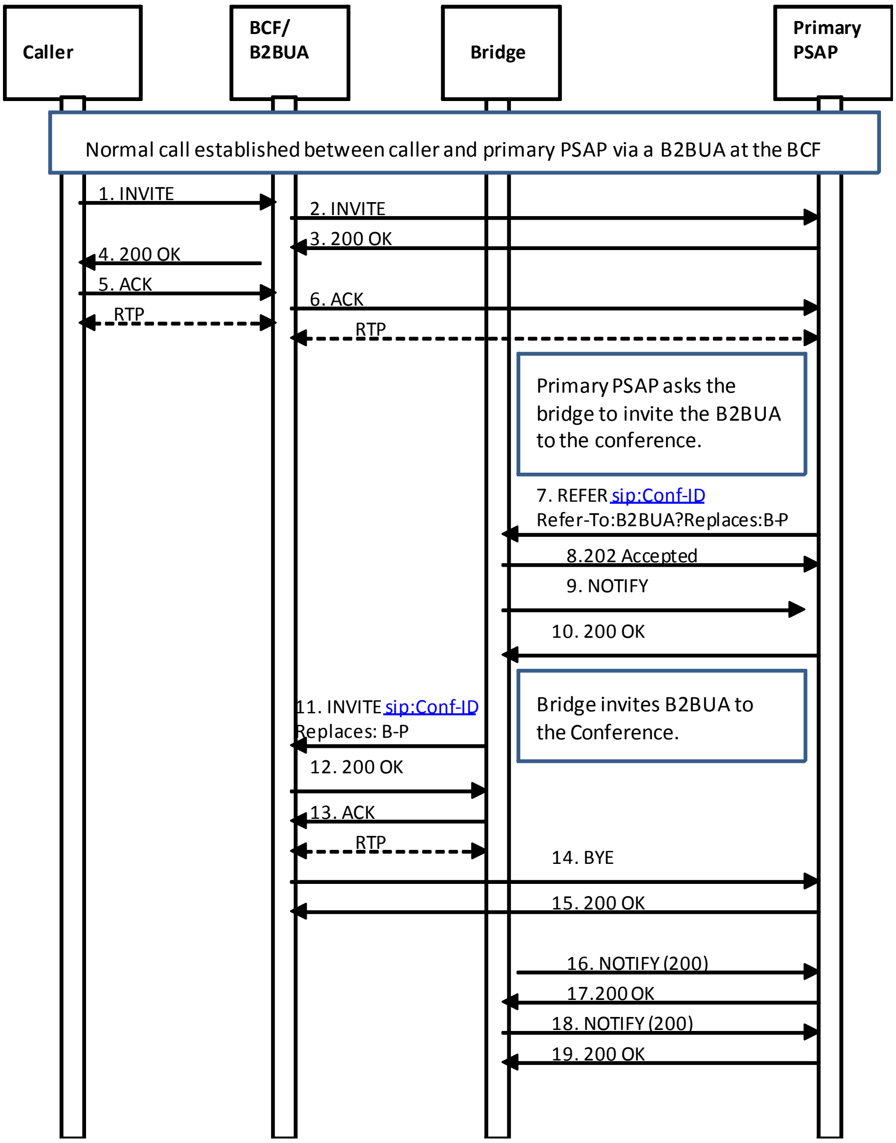
Each of these solutions is specified in more detail in the sections below.

4.9.1 B2BUA in the Border Control Function

When this solution is implemented, the BCF must include a B2BUA function as described in RFC3261. 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 BCF
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 BCF 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.


Caller
BCF/ B2BUA
Bridge
Primary PSAP
Normal call established between caller and primary PSAP via a B2BUA at the BCF
1. INVITE
2. INVITE
3. 200 OK
4. 200 OK
5. ACK
6. ACK
RTP
RTP
Primary PSAP asks the bridge to invite the B2BUA to the conference.
7. REFER sip:Conf-ID Refer-To:B2BUA?Replaces:B-P
8.202 Accepted
9. NOTIFY
10. 200 OK
Bridge invites B2BUA to the Conference.
11. INVITE sip:Conf-ID Replaces: B-P
12. 200 OK
13. ACK
RTP
14. BYE
15. 200 OK
16. NOTIFY (200)
17.200 OK
18. NOTIFY (200)
19. 200 OK

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 ESInet toward the Primary PSAP. (Elements and signaling involved in routing the emergency call within the 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.

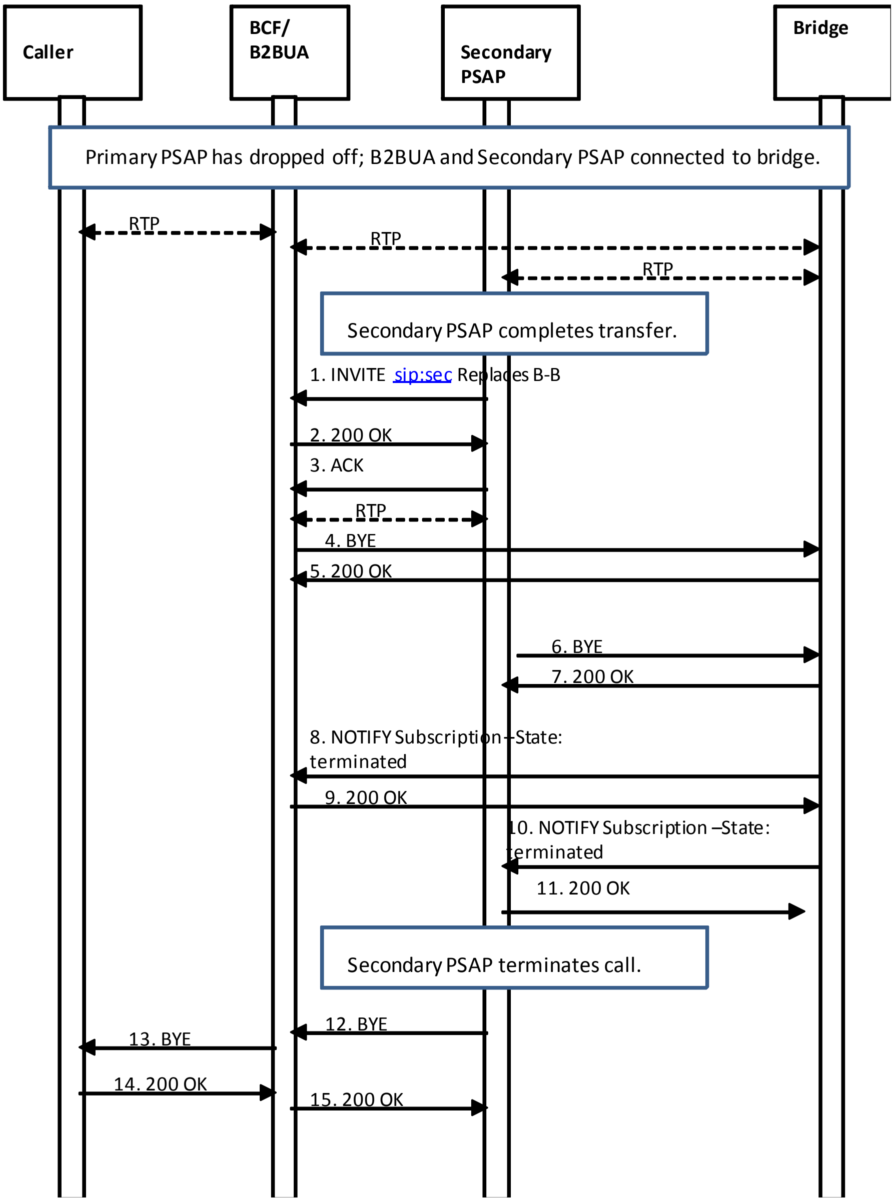
    A media session is established between the B2BUA and the bridge. Note that the media session between the B2BUA and the Primary PSAP still exists at this time. Note also that the media session between the caller and the B2BUA is undisturbed. As above, the B2BUA may cross connect media from the caller 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 5.7.1.3. Once the Primary PSAP determines that the transfer can be completed, it drops off the call, following the flow described in Section 5.7.1.4. 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.


Caller
BCF/ B2BUA
Secondary PSAP
Bridge
Primary PSAP has dropped off; B2BUA and Secondary PSAP connected to bridge.
RTP
RTP
RTP
Secondary PSAP completes transfer.
1. INVITE sip:sec Replaces B-B
2. 200 OK
3. ACK
RTP
4. BYE
5. 200 OK
6. BYE
7. 200 OK
8. NOTIFY Subscription–State: terminated
9. 200 OK
10. NOTIFY Subscription –State: terminated
11. 200 OK
Secondary PSAP terminates call.
12. BYE
13. BYE
14. 200 OK
15. 200 OK

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 "Additional Data associated with a PSAP" data structure.
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:

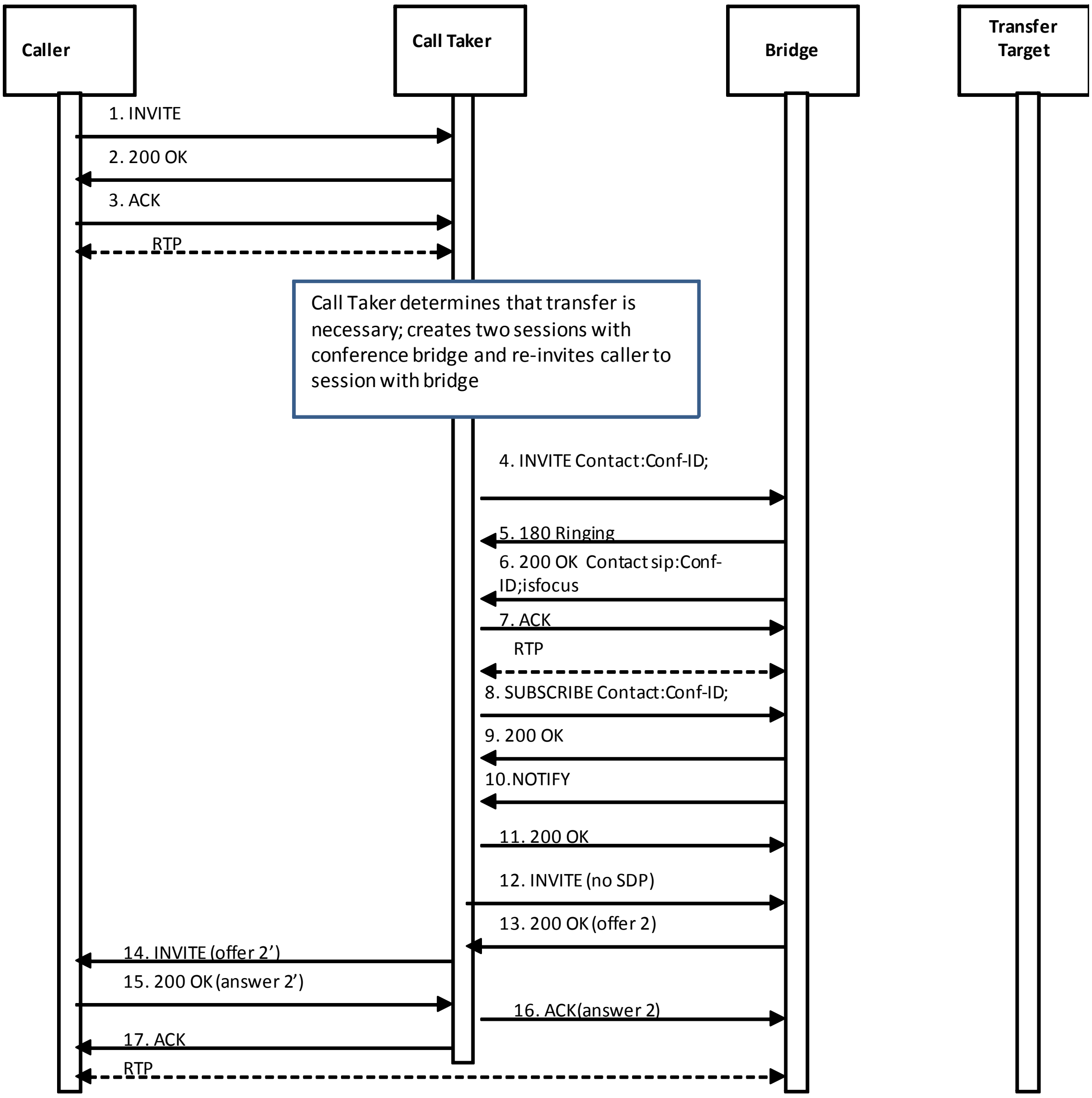
- The solution is deployed at the edge of the ESInet; the rest of the ESInet can assume Replaces works
- Media is anchored at the BCF regardless of what happens to the call

- The B2BUA is call stateful.
- The B2BUA is in the path regardless of whether the device implements Replaces or not.

4.9.2 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.

4.9.2.1 Call Taker Creates a Conference


Caller
Call Taker
Bridge
Transfer Target
1. INVITE
2. 200 OK
3. ACK
RTP
Call Taker determines that transfer is necessary; creates two sessions with conference bridge and re-invites caller to session with bridge
4. INVITE Contact:Conf-ID;
5. 180 Ringing
6. 200 OK Contact sip:Conf-ID;isfocus
7. ACK
RTP
8. SUBSCRIBE Contact:Conf-ID;
9. 200 OK
10.NOTIFY
11. 200 OK
12. INVITE (no SDP)
13. 200 OK (offer 2)
14. INVITE (offer 2')
15. 200 OK (answer 2')
16. ACK(answer 2)
17. ACK
RTP

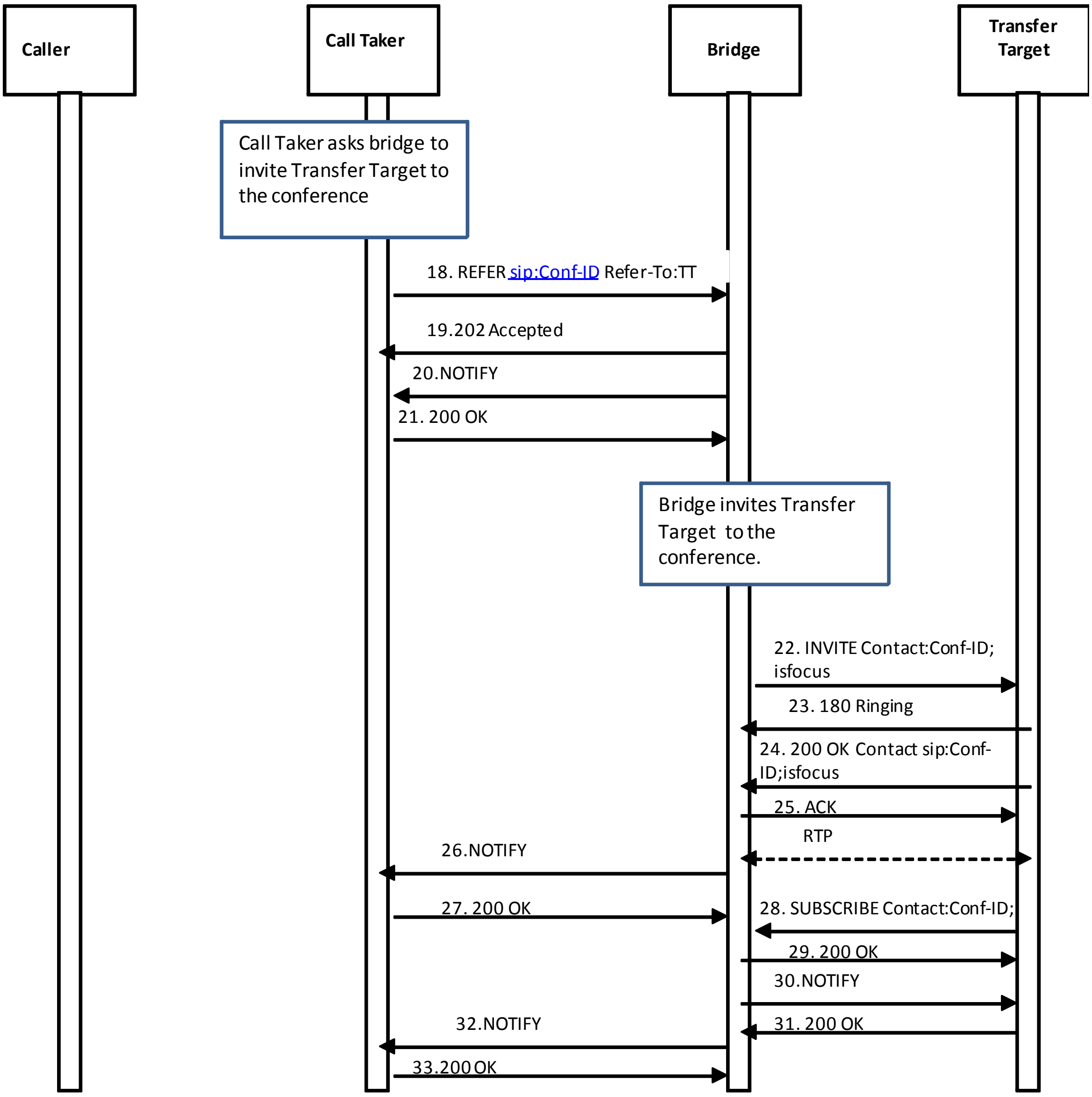
1. The caller initiates an emergency session request by sending an INVITE message via the ESInet to the Primary PSAP call taker. The INVITE contains a Geolocation header with caller location information. (Elements and signaling involved in routing the emergency call within the ESInet are not shown in 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 4.8.1.1).

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.

4.9.2.2 Call Taker Asks the Bridge to Invite the Transfer Target to the Conference


Caller
Call Taker
Bridge
Transfer Target
Call Taker asks bridge to invite Transfer Target to the conference
18. REFER sip:Conf-ID Refer-To:TT
19.202 Accepted
20.NOTIFY
21. 200 OK
Bridge invites Transfer Target to the conference.
22. INVITE Contact:Conf-ID; isfocus
23. 180 Ringing
24. 200 OK Contact sip:Conf-ID;isfocus
25. ACK
RTP
26.NOTIFY
27. 200 OK
28. SUBSCRIBE Contact:Conf-ID;
29. 200 OK
30.NOTIFY
31. 200 OK
32.NOTIFY
33.200 OK

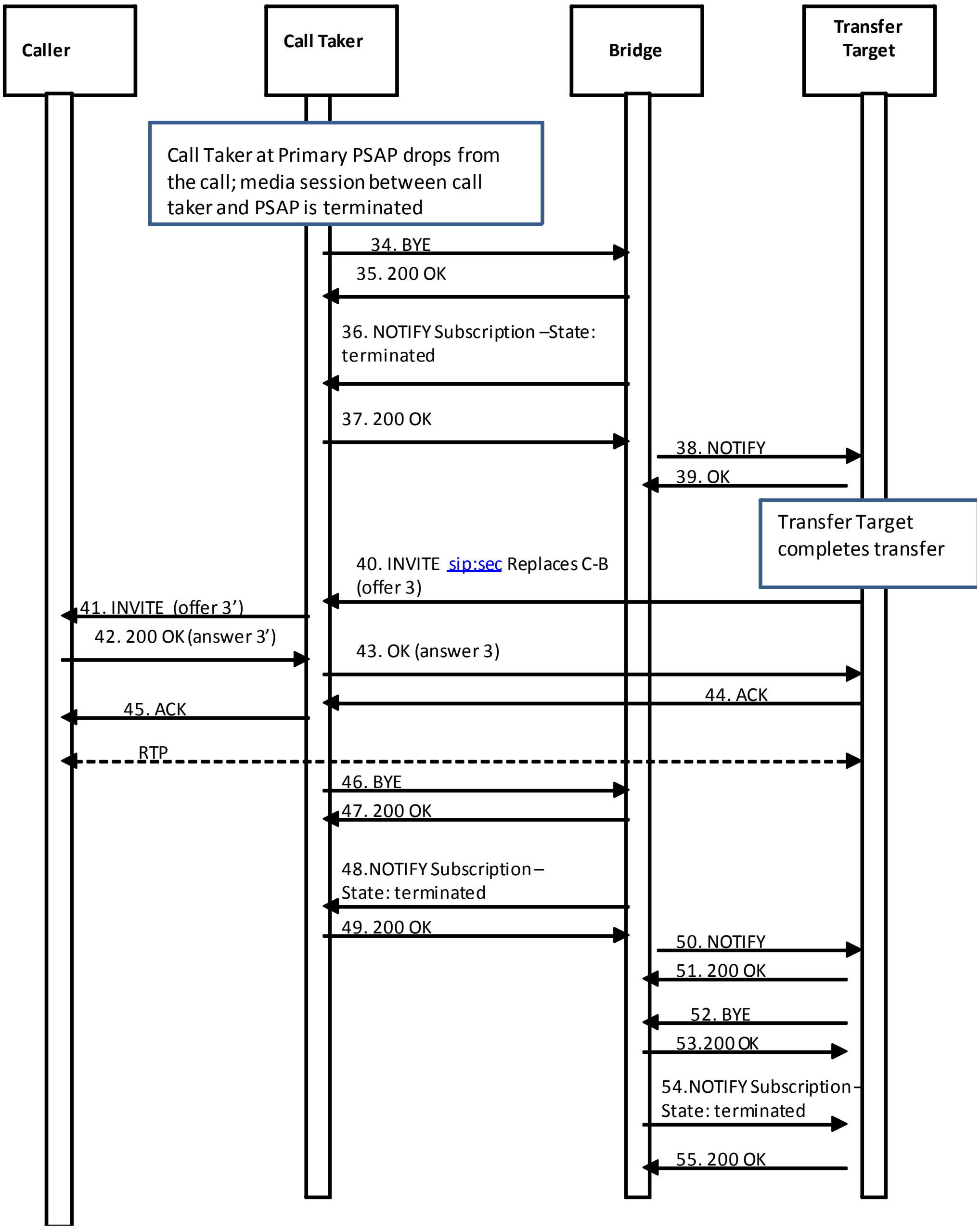
18. The Primary PSAP sends a REFER method to the conference bridge asking it to invite the Transfer Target (i.e., Secondary PSAP) to the conference. The REFER method contains the Conf-ID and a Refer-To header that contains the URI of the Transfer Target. The REFER method also contains an escaped Call-Info header field containing a reference URI that points to the "Additional Data Associated with a PSAP" data structure.
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 "Additional Data Associated with a PSAP" data structure.
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.

4.9.2.3 Primary PSAP Drops; Transfer Target Completes Transfer


Caller
Call Taker
Bridge
Transfer Target
Call Taker at Primary PSAP drops from the call; media session between call taker and PSAP is terminated
34. BYE
35. 200 OK
36. NOTIFY Subscription –State: terminated
37. 200 OK
38. NOTIFY
39. OK
Transfer Target completes transfer
40. INVITE sip:sec Replaces C-B (offer 3)
41. INVITE (offer 3')
42. 200 OK (answer 3')
43. OK (answer 3)
44. ACK
45. ACK
RTP
46. BYE
47. 200 OK
48.NOTIFY Subscription – State: terminated
49. 200 OK
50. NOTIFY
51. 200 OK
52. BYE
53.200 OK
54.NOTIFY Subscription-State: terminated
55. 200 OK

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.

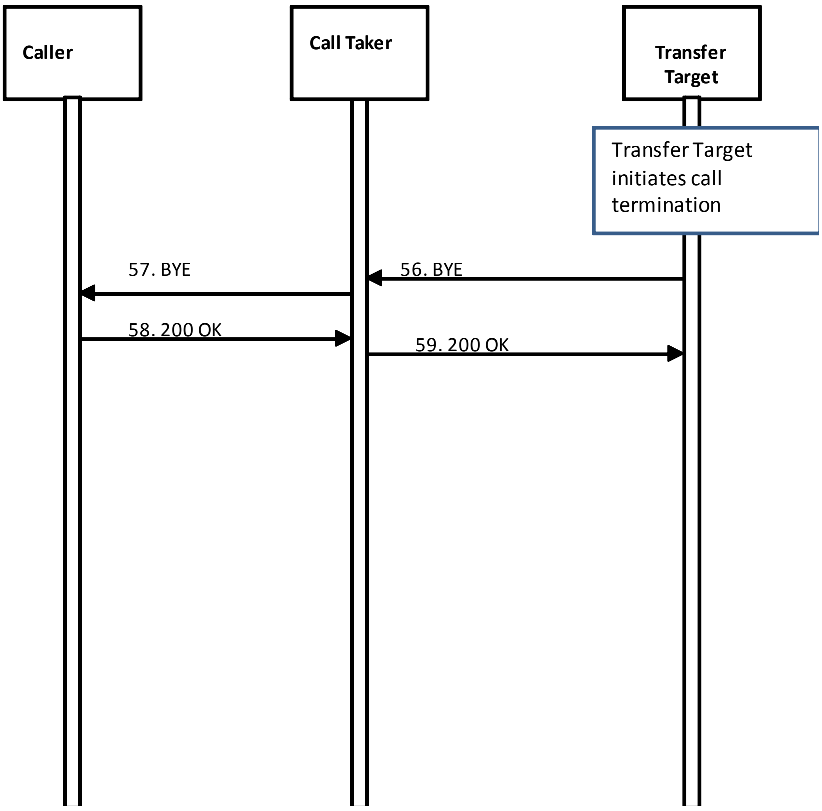
At this time the media session between the caller and the bridge is terminated.

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.

4.9.2.4 Transfer Target Terminates Session with Caller



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. 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.

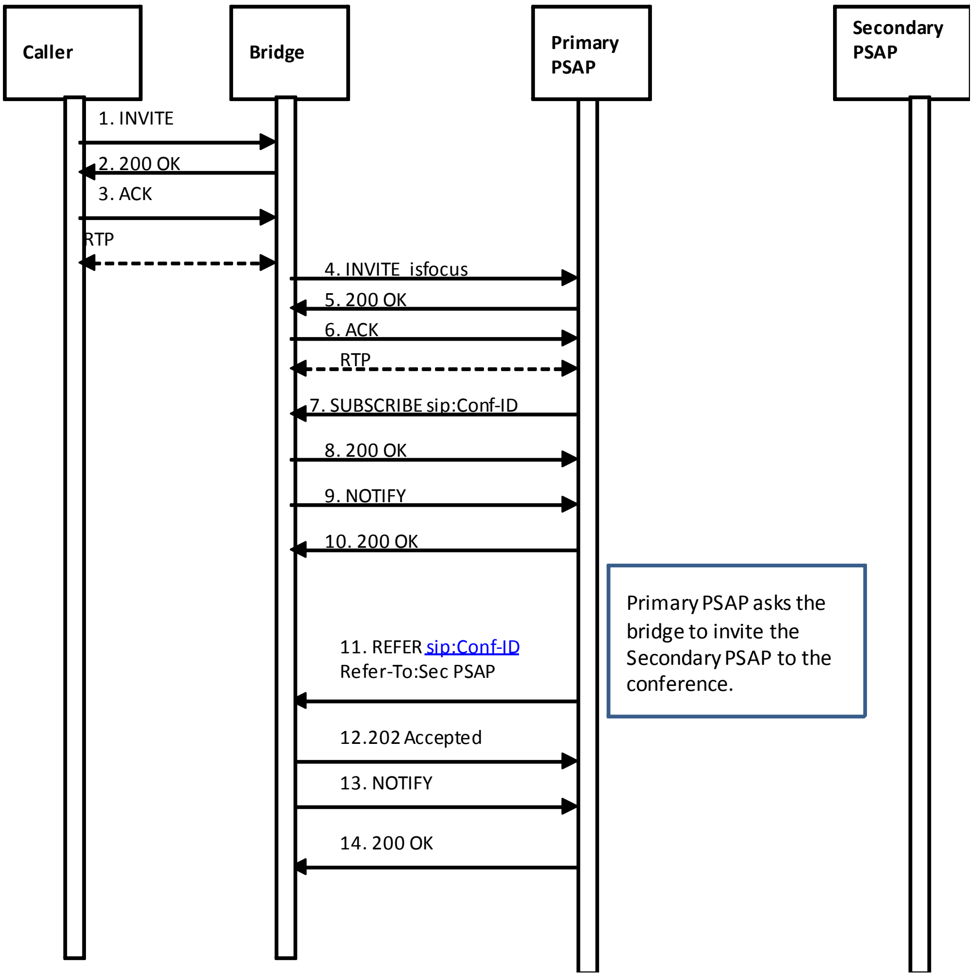
The characteristics of this solution are:

- No additional network signaling elements in the path unless necessary
- Media goes direct between endpoints
- Caller UA receives multiple Re-INVITE messages

4.9.3 Answer all calls at a bridge

All incoming 112 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.

4.9.3.1 Call Established Between Caller and Primary PSAP Via Bridge; Primary PSAP Asks Bridge to Invite the Secondary PSAP to the Conference



1. The caller initiates an emergency session request by sending an INVITE message into the ESInet. The INVITE contains a Geolocation header with caller location information. (Elements and signaling involved in routing the emergency call within the ESInet are not shown in this flow.) The call is routed using mechanisms, and the URI of the target Primary PSAP is determined. The call is delivered to a bridge in the 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 message generated by the bridge must include a Geolocation header that contains the caller location information received in the Geolocation header of the INVITE message from

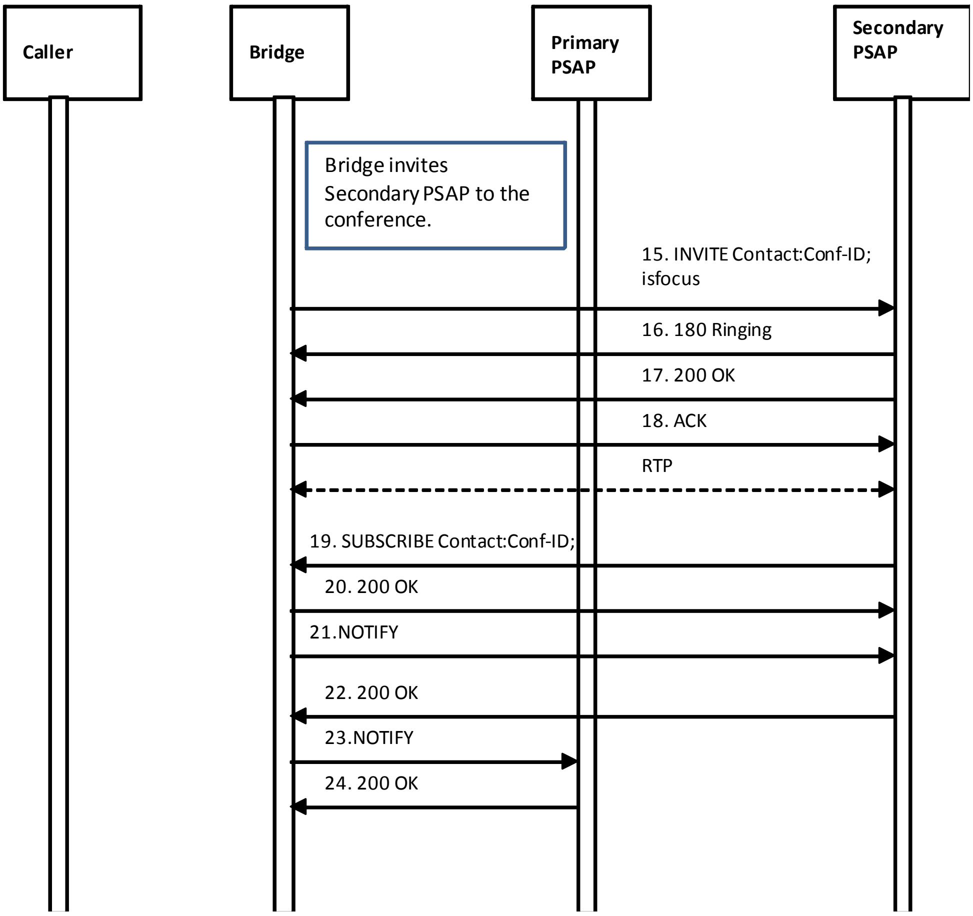
the caller, as well as any Call-Info headers that were received in the incoming INVITE message.

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 contains an escaped Call-Info header field containing a reference URI that points to the "Additional Data Associated with a PSAP" data structure.
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).
14. The Primary PSAP returns a 200 OK in response to the NOTIFY message.

4.9.3.2 Bridge Invites the Secondary PSAP to the 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 containing a reference URI that points to the "Additional Data Associated with a PSAP" data structure.
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.

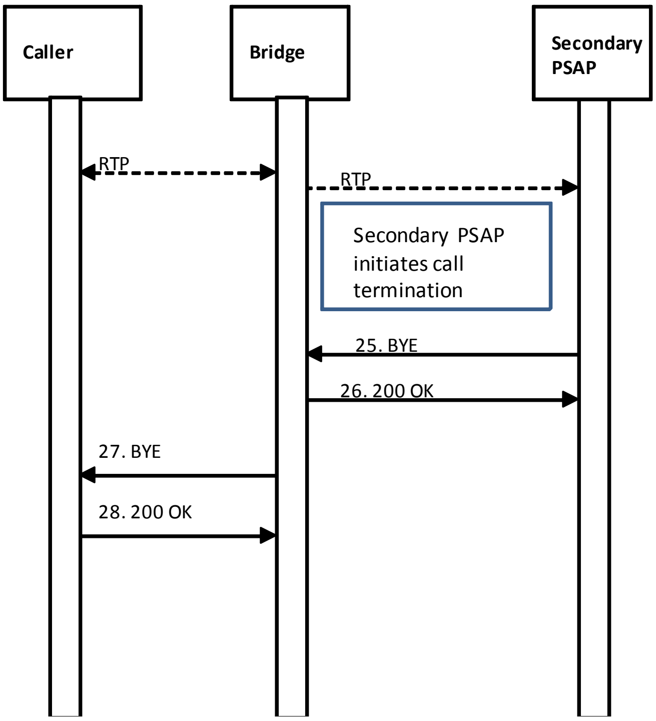
    A media session is established between the Secondary PSAP and the bridge.
19. The Secondary PSAP subscribes to the conference associated with the Conf-ID provided in the INVITE message from the bridge by sending a SUBSCRIBE message to the bridge.

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.

4.9.3.3 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 5.7.1.4. When the Secondary PSAP determines that the call should be terminated, it will follow the flow illustrated below.



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 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 headers 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 call taker's system behaves differently in this scenario in that the initial call is received with an 'isfocus' feature parameter; call taker need not establish a bridge if it determines that a transfer is necessary

4.9.4 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.

4.10 Location Information Server (LIS)

A Location Information Server supplies location, in the form of a PIDF-LO (location by value) or a location URI (location by reference). The LIS also provides a "dereference" service for a location URI it supplies: given the URI, the LIS provides the location value as a PIDF-LO. A LIS may be a database, or may be a protocol interworking function to an access network specific protocol.

In NG112, the LIS supplies location (by value or reference) to the endpoint, or 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 PSAP may dereference a location URI as part of processing a call.

If the LIS supplies location by reference, it must support HELD [9] 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 [103] and event rate control [113].

LISs queried by Legacy Network Gateways during the processing of a wireline emergency call would typically use HELD with the identity extension [104] using a telephone number as the identity and supply location by value in return.

LISs queried by Legacy Network Gateways during the processing of wireless emergency calls are usually protocol interwork functions between SIP or HELD and the legacy network's location determination subsystem. Typically they would supply location by reference.

If the broadband 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.

A LIS must validate locations prior to entering them in to the LIS using the LVF (Section 4.5).

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. Whether the reference should remain valid for some time beyond the duration of the call is a topic for future study as are the privacy considerations of such access.

4.11 Call Information Database (CIDB)

A call that passes through an origination network or service provider of any kind must have a Call info header with a URI that resolves to an AdditionalCall Data structure. The database that dereferences this URI is a Call Information Database.

All origination networks and service providers (where a service provider here is a 3rd party in the path of a call which is not the originating network presenting the call to the ESInet) are required to provide at least this minimum set of information which must be populated in a CIDB. The CIDB is queried with the URI obtained from the Call-Info header with a purpose of emergencyCallData, and returns the

Additional Call Data structure. The query is an HTTPS GET with the URI obtained from the Call-Info header. The return is the XML data structure. It is important that ALL service providers handling the call add a Call-Info header and supply a CIDB to dereference it. The transaction to dereference the Additional Call Data URI must be protected with TLS. The dereferencing entity, which may be an ESRP, PSAP or responding agency uses its credentials. The service provider can use any credential, as long as the domain listed in the URI is the domain of the SubjectAltName in the cert.

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

Devices such as telematics equipped vehicles and medical monitoring devices that can place emergency calls should have the capability to respond to a CIDB query, which includes the reference to the device data (telematics, health monitoring, …). A service provider (such as a telematics service provider) may provide the CIDB instead of the device. Other devices may also provide a CIDB for use in an emergency call.

More information about the additional data structure can be found in [144]

4.12 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 [134]. 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 5.1.8

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 Section 4.3.1.2 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.

4.13 Logging service

The logging service in NG112 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. NG112 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.

4.13.1 Interfaces

The log service is primarily a web service. In addition to the web service interface, logging services that record media provide an RTSP (RFC 2326 [135]) interface to play back the media. The web service includes the following functions.

4.13.1.1 LogEvent

LogEvent logs an event into the logging service. The LogEvent includes parameters:

Parameter	Type	Description
timestamp	String	A timestamp
agencyOrElement	String	agencyID or hostname of an element which logged the event
agent	String	The agentId of an agent at the agency listed in the agentOrElement tag
callId	String	The call identifier of a call
incidentId	String	The Incident Tracking Identifier associated with the call
eventext phonespe	Enumeration	Type of log record

Each Eventext phonespe contains additional data specific to the Eventext phonespe.

The following Eventext phonespes are defined in this document

CallProcess: Each element, which is not call stateful, but handles a call logs the fact that it saw the call pass through by logging a CallProcess event. There are no parameters to "Call Process"

StartCall/EndCall: Each element which is call stateful logs the beginning and end of its processing of a call with Start Call and End Call events. StartCall includes a copy of the headers in the INVITE message, encoded in <header> tags. EndCall includes the response code that ended the call (200 OK in the case of a successful call), encoded in a <responseCode> tag.

Note: it may be desirable to log other messages that are part of the INVITE transaction, such as the ACK. This will be covered in a future edition of this document.

TransferCall: When a call is transferred, the transferor, i.e. the PSAP that had the call prior to transferring it, logs it. The transfer target URI is logged in a <transferTarget> tag.

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 Eventext phonespe. The URI where it decided to send the call (encoded in a <uri> tag, plus a text string <reason> for choosing that route is included in the LogEvent. For ESRPs, the name of the rule is included in a <rule> tag.

Media: Media is the log of call media (voice, video and interactive text). The media event includes a text string <udp> tag that contains an RFC 2327 Session Description Protocol [55] description of the media. The SDP must include SDES keys if the RTP stream is protected with SRTP. Each independent stream must include an RFC 4574 [136] label to identify each stream and the label must be logged with a <mediaLabel> tag. More than one Media event can occur for a call. Recorded media streams include integral time reference data within the stream.

EndMedia. EndMedia causes the logging service to terminate recording of media. The EndMedia event includes one or more <mediaLabel> tags, which must match the SDP labels in the corresponding Media event. More than one EndMedia (with different <mediaLabel>s) may occur for a call.

Message: An SIP Message (Instant Message) is logged with a Message log event. The text of the message is included as a <text> parameter.

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 <agency> tag which is an Agency Identifier. Among other uses, PSAP management to query all logging services that may have records about a call or incident uses this event.

Note: a mechanism to discover the logger associated with an agency will be provided in a future edition of this document

MergeIncident: at some point in processing, an agency may determine that a call marked with an IncidentId may in fact be part of another, previously determined Incident. When it is determined that two IncidentIds have been assigned for the same real world Incident, the Ids are merged with MergeIncident. The MergeIncident record contains the IncidentId of the incorrectly assigned incident in the <incidentId> tag in the header of the log record, and the Incident Id of the actual Incident in an <actualIncident> tag. Note that other agencies may not know that the Incidents are being merged, and therefore could log events against the originally assigned IncidentId.

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

ECRFquery: any element that queries the ECRF and the ECRF itself generate an ECRFquery LogEvent. The LogEvent includes the PIDF-LO (and only the Location Object) using the RFC4119 tags and the service URN in a <service-urn> tag.

ECRFresponse: Both the elements that query the ECRF and the ECRF generate the ECRFresponse. The entire response is logged using the LoST tags.

This document creates a registry for LogEvents. See Section 13.7.

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 "_LI_, 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 _LI_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.

4.13.1.2 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 <logIdentifer> parameter, as returned by the original LogEvent.

When the event is a Media event, the returned event from RetrieveLogEvent will not have the SDP parameter, but will instead have an <rtsp> parameter that must be an RTSP URL. The RTSP URL can be used to play back the media stream(s).

An <errorCode> is also returned from RetrieveLogEvent that can include:

Error Codes

100	Okay No error
517	No such logIdentifier
504	Unspecified Error

Policy controls that can retrieve logged events from the logging service. The policy of the element/agency, which logged the event, governs.

4.13.1.3 ListEventsByCallId

Returns a list of LogIdentifiers that have a specified Call Identifier. The request includes the <callIdentifier>. The response includes zero or more <logIdentifier>(s). An <errorCode> is also returned that can include:

100	Okay No error
518	No such callIdentifier
504	Unspecified Error

4.13.1.4 ListEventsByIncidentId

Returns a list of LogEvents that have a specified Incident Tracking Identifier. The request includes the <incidentIdentifier>. The response includes zero or more <logIdentier>(s). An <errorCode> is also returned that can include:

100	Okay No error
519	No such incidentIdentifier
504	Unspecified Error

4.13.1.5 ListCallsbyIncidentId

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

100	Okay No error
519	No such incidentIdentifier
504	Unspecified Error

4.13.1.6 List IncidentsByDateRange

Returns a list of Incident Tracking Identifiers occurring within a time/date range. The request includes a <startTime> timestamp and an <endTime> timestamp. The response includes zero or more <incidentIdentifier>(s). An <errorCode> is also returned that can include:

100	Okay No error
519	Bad Timestamp
520	EndTime occurs before StartTime
504	Unspecified Error

4.13.1.7 ListIncidentsByLocation

Returns a list of Incidents that occurred within a specified geographic region. The request includes a GML shape in a <areaOfInterest> tag. The response includes zero or more <incidentIdentifier>(s). An <errorCode> is also returned that can include:

100	Okay No error
521	Bad Geoshape
504	Unspecified Error

4.13.1.8 ListIncidentsByDateAndLocation

A combination of ListIncidentsbyDateRange and ListIncidentsByLocation, the request includes a <startTime>, <endTime> and <areaOfInterest>. The response includes zero or more <incidentIdentifier>(s).). An <errorCode> is also returned that can include:

100	Okay No error
519	Bad Timestamp
520	EndTime occurs before StartTime
521	Bad Geoshape
504	Unspecified Error

4.13.1.9 ListCallsByDateRange

Returns a list of Call Identifiers occurring within a time/date range. The request includes a <startTime> timestamp and an <endTime> timestamp. The response includes zero or more <callIdentifier>(s). An <errorCode> is also returned that can include:

100	Okay No error
519	Bad Timestamp
520	EndTime occurs before StartTime
504	Unspecified Error

4.13.1.10 ListAgenciesByCallId

Returns a list of agencies that recorded AdditionalAgency events about a call. The request includes a <callIdentifier>. The response includes zero or more <agencyIdentifier>(s). An <errorCode> is also returned that can include:

100	Okay No error
518	No such callIdentifier
504	Unspecified Error

4.13.1.11 ListAgenciesByIncidentId

Returns a list of agencies that recorded AdditionalAgency events about an Incident. The request includes an <incidentIdentifier>. The response includes zero or more <agencyIdentifier>(s). An <errorCode> is also returned that can include:

100	Okay No error
519	No such incidentIdentifier
504	Unspecified Error

4.13.2 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 4.13. 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.

4.13.3 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 NG112 functional elements must have access to a conformant logging service and log all relevant events in it. Media is recorded by the entity answering the call, and by any bridge in the path. 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.

4.13.4 Operational Considerations

To be supplied in a future edition of this standard.

4.14 Forest Guide

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

4.14.1Functional 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 which is authoritative for a subregion 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 NG112, each state is a tree, with local ECRF/LVFs as the children. The top of the tree is a state ECRF/LVF. There is a national forest guide that has knowledge of the state trees. The national forest guide exchanges mappings with other national forest guides. A state mapping, exported to the national forest guide is the civic state element, and a polygon representing the state boundary (or more precisely, the union of the coverage regions of all PSAPs in the state).

4.14.2 Interface Description

The national forest guide maintains a LoST interface, as described in Section 5.5, for query resolution. It also maintains a LoST-sync interface defined in [112] 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:EES:service:sos and urn:EES:service:responder. It may be able to refer to other forest guides for services other than these.

4.14.3Data Structures

The Forest Guide has a civic data structure (PIDF-LO down to the A2 level) and a GML polygon (set) representing the state coverage region. It also maintains mappings for other countries in a similar manner (civic A1 level, plus a polygon set for the country coverage region).

4.14.4Roles and Responsibilities

The Forest Guide must be managed nationally and may evolve to an entity more representative of all public safety agencies. State ECRF and LVF operators are responsible to arrange for their mappings 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.

4.14.5Operational Considerations

While the national forest guide is only authoritative for the service urns listed above, it may refer other queries to other forest guides if it knows the forest guide for that service. 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 deciding what is an authoritative forest guide for another country or area. Specifically, it can be expected to have to deal with disputed territory, where more than one national forest guide claims they are authoritative for the same area.

4.15 DNS

All elements identified by hostnames must have corresponding Domain Name Service (DNS) records STD13 [106] 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.

A domain that has SIP elements within the domain must have an SRV record RFC 2782 [107] for a SIP service for the domain, and any of its subdomains which may appear in a URI.

4.16 Agency Locator

To be provided in a future edition of this document.

4.17 Policy Store

4.17.1Functional Description

A policy store holds policies created by an agency and used by a functional element such as an ESRP. The policy store is a simple repository; it does not manipulate the policy.

4.17.2Interface Description

A policy store implements the policy storage and retrieval functions defined in Section 5.4.1. Policy store replicas can be maintained by having one policy store retrieve policies from another policy store and subsequently accept requests to retrieve such policies. Replicas normally do not allow a policy store operation for a policy that they replicate. There is always one (possibly redundant) authoritative policy store for a given policy.

4.17.3Roles 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, and the element must have a mechanism to not use the internally stored replica, but rather retrieve the policy from the authoritative source if provisioned to do so.

4.18 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 timeserver, which may have a hardware clock if it is more accurate than syncing the server to the ESInet timeserver.

4.19 Origination Networks and Devices

A device, network or service provider presenting calls to an ESInet must 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.

4.19.1SIP Call Interface

The origination network must present calls to the ESInet meeting the ESInet SIP interface specified in Section 5.1. All calls must 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.

4.19.2Location by Reference

Origination networks that are also access networks must also provide a Location Information Server function (that is, location dereference, and location validation if applicable) meeting the requirements of Section 4.10 if they supply location by reference.

4.19.3Call Information Database

Origination networks and devices presenting calls to ESInets must provide a Call Information Database interface meeting the requirements of Section 4.11.

4.20 PSAP Callbacks

Two concepts can be considered as callbacks:

1. After an emergency call is completed (either prematurely terminated by the emergency caller or normally by the call taker) it is possible that the call

taker feels the need for further communication. For example, the call may have been dropped by accident without the call taker having sufficient information about the current situation of a wounded person. A call taker may trigger a callback towards the emergency caller using the contact information provided with the initial emergency call. This callback could, under certain circumstances, be treated like any other call and as a consequence it may get blocked by authorization policies or may get forwarded to an answering machine.

The IETF emergency services architecture specification [59] already offers a solution for allowing PSAP callbacks to bypass authorization policies to reach the caller without unnecessary delays. Unfortunately, the specified mechanism only supports a limited set of use cases. To extend the support for callback an additional specification [154] provides additional functionality for PSAP callbacks. [154] allows a PSAP to mark calls as callbacks and those marked calls receive preferential treatment.

2. Occasionally, when on an emergency call, a caller hangs up the call before the call taker is finished acquiring enough information.

   Emergency calls are stressful, and mistakes are inevitability made. A mechanism is needed to re-establish communication between the caller and the call taker when this happens. The PSTN has a feature available, "Called Party Hold" (CPH), which is used in some PSAPs to meet this requirement. If the user hangs up the call is not torn down, but instead is maintained. If the handset is picked up, since the call is still active and resources maintained, the caller and the call taker are readily reconnected. Called Party Hold is a feature that has long been available in wireline networks, but is not currently implemented in wireless networks. Some PSAPs are desirous of maintaining their current PSAP call disconnect control capability, while other jurisdictions would like to regain access to those capabilities. Still, in other PSAPs, the function may not be needed or desired, even in jurisdictions that want to have the feature, it may not be desirable in all circumstances.

   Standardization for handling abandoned calls and premature disconnects in IP-based networks work has been suggested and can be found in [175]. Note that this work has not found additional support in standards organizations yet and may therefore not be available in deployments.

5 Interfaces

5.1 SIP Call

The call interface is SIP [12]. All calls presented to the ESInet must be SIP signaled. Calls are potentially multimedia, and can include one or more forms of media (audio, video and/or text[11]). See Section 5.6 for a discussion of "non-human-associated calls" which can be used for non-human-associated requests for help where there is no human caller. SIP is also the protocol used to call a 112 caller back, and for calls between agents within the ESInet.

SIP is a complex protocol defined in a large number of standards documents. All NG112 elements which process calls must implement all of the standards listed in Section 3 (Core Standards) in the "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 112 call just because it doesn't meet some standard detail if it's reasonably possible to process the call anyway.

There are three primary entities in a SIP protocol exchange:

1. The User Agent Client, which is the initiator of a "transaction" within SIP. In the origination of a 112 call, the calling party's end device is the UAC
2. The User Agent Server, which is the target of a transaction within SIP. In the origination of a 112 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 112 call, the calling party's carrier may have two or more proxies. The ESInet has at least one proxy (an Emergency Services Routing Proxy) and typically has more than one.

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.

[11] 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.

5.1.1 Minimal Methods needed to handle a call

The only method absolutely required to handle a 112 call is the INVITE. The REFER method (defined in [23]) should also be supported 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.

NG112 elements that process 112 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 4.2).

5.1.1.1 INVITE (initial call)

The INVITE method is used to initiate a call. The standard INVITE/OK/ACK sequence must be followed, with allowance for intermediate (1XX) responses. It is generally unacceptable to refuse an INVITE request unless the PSAP is under active attack and cannot respond.

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 would route to the primary PSAP.

The external (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 112 Authority. One strategy is simply to use a general URI that leads to a country level ESRP, for example 112@example.fi. The country ESRP would query the internal (within the ESInet) ECRF with a mapped (from the incoming service URN in the Request URI) service urn, for example urn:EES: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, sip:psap@helsinki.example.fi. This URI would still route to the same country-level ESRP, which would perform the same ECRF query. However, failures at the country 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 ESInet gets some form of "call treatment". Minimal call treatments defined include:

1. Queue a call for answering by a call taker
2. Return Busy (600 Busy Everywhere)
3. Answer at an Interactive Multimedia Response system
4. Divert to another PSAP.

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

All calls that will go to a call taker are queued; however, the time in queue may be negligible.

The PSAP should normally only return a 183 In Progress intermediate response when a 112 call is queued for answer. It is recommended that no other 1XX response be used due to uneven implementations of these responses. 183 In Progress should be repeated at approximately 3 seconds interval if the call is not answered. When placing a callback, 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.

112 calls are usually not redirected, and thus 3XX responses are normally not used; however 3XX may be used for calls within the ESInet. NG112 elements that initiate calls within the ESInet should appropriately respond as defined in RFC 3261 [12]. A 112 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**
183 (Ringing)	A 112 call is queued for answer. It is recommended that no other 1XX response be used due to uneven implementations of these responses. 183 Ringing should be repeated at approximately 3 second intervals if the call is not answered.
200 (OK)	Normal response to an answered call
3XX	112 calls are usually not redirected, and thus 3XX responses are normally not used. 3XX may be used for calls within the ESInet. NG112 elements that initiate calls within the ESInet should appropriately respond as defined in RFC 3261 [12].
400 (Bad Request)	A 112 call is so malformed that the BCF cannot parse the message.
401	Should never occur for a 112 call, but proxy authorization is required for all calls originated by entities within an ESInet.
402	Should never occur for a 112 call or an internal call
403 (Forbidden)	Normally, 403 (Forbidden) should not occur, but if the BCF passes a malformed INVITE which downstream devices cannot handle, they may have no choice but to return 403.
404 (Not Found)	404 (Not Found) would normally not occur for a 112 call, but may be used within the ESInet.

406 (Not Acceptable)	The 406 (Not Acceptable) should not occur for a 112 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 (Request Timeout)	May be issued in an unplanned circumstance. Normally, this should never happen to a 112 call.
413 (Request Entity too Large)	The BCF should accept any Request URI, but downstream elements may return 413 (Request Entity Too Large).
414 (Request-URI Too Long)	The BCF should accept any Request URI, but downstream elements may return 414 (Request-URI Too Long).
416 (Unsupported URI Scheme)	The BCF should accept any Request URI, but downstream elements may return 416 (Unsupported URI Scheme).
486 (Busy Here)	PSAPs may limit the number of test calls, and if that limit is exceeded, the response shall be 486 Busy Here.
600 (Busy Everywhere)	If the BCF detects an active attack, it should respond with 600 (Busy Everywhere), rather than another 4XX response.

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 "reINVITE" in SIP. Re-INVITEs may be used on any call within the ESInet, including a 112 call. ReINVITE may be initiated from either end of the call. Note that when the reINVITE is initiated by the called party, it becomes the UAC and the calling party becomes the UAS.

5.1.1.2 REFER (transfer)

The REFER method is used with 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 the calling device supports REFER, the REFER can be sent to the calling device to transfer a call. Section 4.9 discusses the problem of a calling device that is unable to support a REFER transaction.

5.1.1.3 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.

Note: There is a requirement to allow PSAPs to optionally control disconnect. There are no standards that describe how this is accomplished in SIP signaling, but discussion on the subject is ongoing in the IETF ecrit work group and appropriate work in other SDOs will be required. A future edition of this document is expected to describe how PSAP control of disconnect is implemented.

5.1.2 Methods allowed to be initiated by caller which must be supported

5.1.2.1 CANCEL (cancel call initiation)

An attempt to create a call with INVITE may be cancelled before it is completed with a 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 ESInet elements must treat a CANCELled call as such, including logging requirements.

5.1.2.2 UPDATE (update parameters)

UPDATE is defined in RFC3311 [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 reINVITE. UPDATE may be used on any call within an ESInet (including 112 calls).

5.1.2.3 OPTIONS (option negotiation)

Options may be used by an external caller, or inside the ESInet to determine the capabilities of the destination UA. All endpoints within the ESInet must be capable of responding to an OPTIONS request, as defined in RFC3261. It would be unusual, but not improper, for an external caller to query the PSAP with OPTIONS before placing an emergency call.

An OPTIONS transaction is the preferred mechanism for maintaining a "keep alive" between two SIP elements. Periodic OPTIONS transactions must be used between ESRPs which normally pass calls between themselves, between the ESRP and the PSAPs and LPGs it normally serves, and between the PSAP and the bridge it normally uses. The period between OPTIONs used for keep-alive should be provisioned, and default to 1 minute (which must be less than the TLS timeout period) intervals during periods of inactivity. Since OPTIONs requires an exchange of messages, only one member of a pair of "adjacent" SIP elements need initiate OPTIONS towards the other.

5.1.2.4 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.

5.1.2.5 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 ESInet 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.

5.1.2.6 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. 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 MIME body parts. MESSAGE requests do not themselves initiate a SIP dialog or session. MESSAGE requests may also be sent in the context of a dialog or session initiated by some other SIP request (such as INVITE), for example in a multi-media call or text messaging session. For more information on MESSAGE please refer to RFC 3428 [21]. Non-human-associated calls are sent using MESSAGE requests outside of a session. Text messages or instant messages may be sent using MESSAGE within a session (in which case an interactive associated stream of such messages is established) or outside a session (in which case a set of disconnected stand-alone messages are sent). MESSAGE is part of the SIP/SIMPLE presence and messaging system.

5.1.2.7 INFO

The INFO method is used for communicating mid-session signaling information along the signaling path for a call. INFO is not recommended for use within the

ESInet. However, many video communication implementations are depending on use of INFO for requesting a full video frame when packets have been lost as specified in RFC 5168. It is essential that such use of INFO is supported.

Orderly transition to use of RTCP for media control can be achieved if the procedures of RFC 5104 are supported.

5.1.3 Methods used within the ESInet

5.1.3.1 REGISTER (Call Taker to PSAP "login")

As defined in RFC 3261 [12], any PSAP UA must register with a SIP register server within their domain to ensure that emergency calls can be delivered to them.

5.1.3.2 SUBSCRIBE/NOTIFY (Events)

Subscribe/Notify is a mechanism to implement asynchronous events notification between two elements, 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 RFC3265 [17] Section 7.1

5.1.3.3 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 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 event state. The body of a PUBLISH request carries the PUBLISH event state. For more information refer to RFC 3911 [41].

5.1.4 Headers assumed supported at the interface to the ESInet

All SIP elements within an ESInet should support Robust Header Compression (ROHC) [145]. BCF's must support ROHC.

Note: *The phoneBCP document referenced in this section contains text normative on devices and service providers. This document considers only the interface between an origination network and the ESInet. References to phoneBCP 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 the IETF phoneBCP document, regardless of wording and context in that document, shall apply only to the ESInet 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 ESInet.*

Header	**Defined In**	**See Section (or Phonebcp)**	**Notes**
To	RFC3261 Section 8.1.1.2 & 20.39	ED63 2.	Usually sip:112 or urn:service:sos
From	RFC3261 Section 8.1.1.3 & 20.20	ED63 3.	Content cannot be trusted unless protected by an Identity header
Via	RFC3261 Section 8.1.1.7 & 20.42	ED63 4.	Occurs multiple times, once for each SIP element in the path
CSeq	RFC3261 Section 8.1.1.5 & 20.16		Defines the order of transactions in a session
Call-Id	RFC3261 Section 8.1.1.4 & 20.8		NOT the NG112 call id
Contact	RFC3261 Section 8.1.1.8 & 20.10	ED63 6.	Usually a "globally routable user agent URI" (gruu)
Content-Length	RFC3261 Section 20.14		
Content-Type	RFC3261 Section 8.2.3 & 20.15		Used in, for example, in RFC4119 and RFC4566[12]
Geolocation	RFC6442	ED63 9.	
History-Info	RFC4244		Indicates call has been retargeted
P-Asserted-Identity	RFC3325		When present, overrides From
Reason	RFC3326		Used with History Info to specify why a call was retargeted
Route	RFC3261 Section 20.34	ED63 5.	Usually ESRP/PSAP URI

[12] 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.

Supported	RFC3261 Section 8.1.1.9 & 20.37	ED63 8.	
Replaces	RFC3891	4.8	Used with transfer

5.1.5 Headers Accepted and also used internally

Header	**Defined In**	**Section**	**Notes**
Max-Forwards	RFC3261 20.22		Specifies the maximum number of SIP elements that may be traversed before assuming a routing loop has occurred
Accept	RFC3261 20.1		
Content-Encoding	RFC3261 20.12		
Accept-Encoding	RFC3261 20.2		
Content-Language	RFC3261 20.13		
Accept-Language	RFC3261 20.3		
Content-Disposition	RFC3261 20.11		
Record-Route	RFC3261 20.30		
Allow	RFC3261 20.5		
Unsupported	RFC3261 20.40		
Require	RFC3261 20.32		
Proxy Require	RFC3261 20.29		
Expires	RFC3261 20.19		
Min-expires	RFC3261 20.23		
Subject	RFC3261 20.36		
Priority	RFC3261 20.26		
Date	RFC3261 20.17		
Timestamp	RFC3261 20.38		
Organization	RFC3261 20.25		

User-Agent	RFC3261 20.41	
Server	RFC3261 20.35	
Authorization	RFC3261 20.7	
Authentication-Info	RFC3261 20.6	
Proxy-Authenticate	RFC3261 20.27	
Proxy-Authorization	RFC3261 20.28	
WWW-Authenticate	RFC3261 20.44	
Warning	RFC3261 20.43	
Call-Info	RFC3261 20.9	Used to carry URIs to Additional Call/Caller data
Error-Info	RFC3261 20.18	
Alert-Info	RFC3261 20.4	
In-Reply-To	RFC3261 20.21	
MIME-Version	RFC3261 20.24	
Reply-To	RFC3261 20.31	
Retry-After	RFC3261 20.33	
RAck	RFC3262 7.2	
RSeq	RFC3262 7.1	
Event	RFC3265 7.2.1	
Allow Events	RFC3265 7.2.2	
Subscription-State	RFC3265 7.2.3	
Resource Priority	RFC4412 3.1 Section 4.1.6	

5.1.6 Resource Priority

The resource priority header (RFC4412) 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. BCFs must police Resource Priority for incoming SIP calls. Calls that appear to be 112 calls 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:

esnet.0	Calls which relate to an incident in progress, but whose purpose is not critical
esnet.1	112 calls traversing the ESInet
esnet.2	Calls related to an incident in progress which are deemed critical
esnet.3-esnet.7	not defined

5.1.7 History-Info and Reason

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 ESInet must support the History-Info header (RFC4244 [44]) and the associated Reason header (RFC3326 [22]). Elements, which retarget a call, must add a History-Info header indicating the original intended recipient, and the reason why the call was retargeted. ESInet elements must be prepared to handle a History-Info (and its associated Reason header) added by an element outside the ESInet before presentment to the 112 system.

5.1.8 Media

All call handling elements must support media using RTP (RFC3550 [13]). Each SIP session initiation message or response should describe the media the User Agent is capable of supporting using Session Description Protocol (SDP) (RFC4566 [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 text phones.

5.1.8.1 Audio

All User Agents in the ESInet must support g.711 mu-law and a-law. It is recommended that AMR, AMR-WB, EVRC[138], EVRC-B[139], EVRC-WB[140], and EVRC-NW[141] also be supported.

5.1.8.2 Video

All User Agents in the ESInet must support H.264/MPEG-4 Version 10 video. The Baseline profile must be supported. Scalable baseline profile support is recommended. At least levels 1-3 must be supported.

5.1.8.3 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 [117]). (In turn specifying use of RFC 4103 [118] for the packetization of real-time text). This medium may be used simultaneously with voice and/or video in calls.

5.1.8.4 Text phones

The NG112 architecture assumes that deaf and hard of hearing callers will migrate from text phones to other forms of communication including real time text devices, total conversation devices and various forms of relay services. Textphones in the PSTN are used in some countries in Europe. Although the use of text phone usage is declining, it cannot be assumed that text phones will be completely gone by the time transition to NG112 is completed. Therefore, PSAPs in countries where legacy PSTN textphones are still in use must be capable of receiving calls from text phones.

Legacy textphone tones are very sensitive to distorsion easily occurring in VoIP gateways and on VoIP connections, so it is not recommended to transport PSTN textphone tones in VoIP networks without very careful deployment considerations and by thorough testing. An alternative is to require conversion to/from RTP and Real-Time Text as close as possible to the textphone, e.g., at the point when the call passes the border to IP.

It is possible to have a transcoder in the path of every voice call which would recognize textphone tones, and replace them with RFC 4103 [118] real time text on incoming (with respect to the ESInet) RTP media, and terminate RFC4103 real time text and synthesize textphone tones for outgoing RTP. The transcoder must be compliant with RFC 5369 [119]. It may be practical to place a transcoder at the edge of an ESiNET to serve all endpoints inside that ESiNET.

The transcoder must on the PSTN tone side handle PSTN textphone tones according to ITU-T Recommendation V.18 [149] or the subset of ITU-T Recommendation V.18 that is motivated by the types of textphones existing in the country of installation. Note that PSTN textphone calls can alternate between text and voice in the same call, e.g. to let a user talk, but read the answers.

ETSI EG 202 320 [153] Duplex Universal Text and Speech contain specifications for the different text telepone protocols, and for the composition of gateways between theese PSTN textpohone protocols and IP based text and audio communication.

5.1.9 Text Messaging / Instant Messaging

Text-based communications for NG112 by all call handling elements of an NG112 system is supported in two ways: Real-Time Text (RTT) and Instant Messages (IM) 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 NG112 in the future, specifically XMPP. At this time, the only standardized IM protocol fully specified for supporting emergency IMs within or presented to an ESInet is SIP/SIMPLE.

All call handling elements within the ESInet must support Session Initiation Protocol (SIP) Extension for Instant Messaging (RFC3428 [21]), Indication of Message Composition for Instant Messaging (RFC3994 [120]), The Message Session Relay Protocol (MSRP) (RFC4975 [121]) and Relay Extension for the Message Session Relay Protocol (MSRP) (RFC4976 [122])[13]. PSAPs must be prepared to handle IM as a series of individual MESSAGE transactions as well as a message session via MSRP. MESSAGEs received from the same caller within a configurable time (2-3 minutes nominally) should be considered part of the same "call", and must be routed to the same PSAP (and the same call taker), regardless of movement of the caller while texting. If the origination network/device supports non session mode IM to NG112, it must assure that all messages from the same caller within this time frame is sent to the same ESInet (same ECRF query results). If the network/device cannot guarantee this, it must use session mode. The ESRP in the ESInet will also maintain a timer for this function and assure that all messages from the same caller that route to an ESInet will route to the same PSAP.

Location must be included in a geolocation header in the MESSAGE method or the initiation of the MSRP session as with any other "call" to 112.

Other Instant Messaging protocols such as XMPP may be supported by an originating network, but must be interworked to SIP IM for presentation to the ESInet. For example, draft-saintandre-sip-xmpp-im-01 [110] describes interwork between XMPP and SIP IM.

5.1.10Non-human-associated calls

Non-human-associated calls are non-interactive calls originated by an automated sensor-based device. Such calls contain data (e.g., sensor data). There is no assumption of a human presence. There may be streaming media (e.g., video or audio feeds). There may be a capability to control the device or another device.

Non-human-associated calls are presented to an ESInet in the same way as regular emergency calls using a SIP INVITE. If these calls only carry data (data-only emergency calls) then the considerations in [TBD] are applicable. In particular, this means that the SIP message contains a Common Alerting Protocol (CAP) [95]

[13] 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.

payload. In addition, the additional data structure [TBD] may provide further information about the call, caller, and location.

Non-human-associated calls are routed and handled the same as voice, video or text calls throughout the NG112 system. The routing mechanisms can route non-human-associated 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 routing function as inputs to direct calls with specified characteristics to specific entities.

5.1.11Bodies in messages.

All SIP elements in an ESInet must support multipart MIME as defined in RFC2046 [123]. For example, location and SDP may be present in a message body. All SIP elements must allow additional body content (for example, images, vcards, etc) to pass to the PSAP. 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 UDP; and may require the use of TCP.

5.1.12Transport

SIP signaling within the ESInet must be TCP with TLS. 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. Fragmentation and reassembly must be supported by all ESInet elements. If TLS establishment fails, fallback to TCP/UDP without TLS is allowed. If fallback with TLS is allowed, 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, which 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 RFC3711 [125] and SDES as defined in RFC 4568 [126]. SRTP security must be requested in all calls originated within an ESInet. Since media is routinely logged, the logger must be given the keys to enable it to decode the SRTP. RTCP as defined in RFC3550 [13] and SRTCP as defined in RFC3711 [125] 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. User Agents who detect the loss of RTP should attempt to reestablish the streams by reINVITING the other party. If that fails, the device should indicate a failure and require the user (call taker in most cases) to take 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 would 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.

5.1.13Routing

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 SRV records [107] will need to be consulted to determine the hostname of the sip server for that domain.

5.1.14Originating network Interface

The originating call interface to the ESInet is a SIP call interface as described above in Section 4.1. All calls are presented to an ESInet by routing via an ECRF or equivalent as described in Section 4.4. 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 message. 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 message, 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.

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.

A Call-Info header must be included in the incoming INVITE message to the ESInet that contains a URI that refers to an Additional Data associated with a Call [144].

5.1.15PSAP 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 (Section 4.3.1.5). Geolocation header, Call-Info headers and other headers should be the same as above (Section 5.1.14). The call will be routed, using normal RFC 3261 [12] procedures to the URI obtained from the ESRP's PRF. See Section 4.7.1 for other information on the PSAP interface.

5.1.16Element 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 [114]. Simple mechanisms to handle overload are insufficient. Elements must not return

503 Busy Here unless it is certain, by design and configuration that the upstream element can reliably cope with the error. This standard specifies specific 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]

5.2 Location

Location is fundamental to the operation of the 112 system. Location is provided outside the ESInet, and the generic functional entity, which provides location is a Location Information Server (LIS). Since the LIS is external to the ESInet, and not provided by the 112 Authority, the LIS is out of scope for this arquitecture. 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 functions a LIS provides that are relevant are:

a) A dereference function defined below for location by reference
b) A validation function which uses the LVF for civic addresses

Any element that provides either or both of these two functions is considered a LIS. 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 NG112 system supports location included by value in a Geolocation header [10] of a SIP message. It also supports location by reference. All elements in an ESInet that use location by reference must implement SIP and HTTP Enabled Location Delivery (HELD) dereferencing protocol. A Location Information Servers (LIS)[14] must implement one or both of these protocols.

Location by reference using SIP is an implied subscription to Presence (RFC3856). An element needing location that has a SIP location URI must issue a SIP SUBSCRIBE (RFC3265) to the location URI. The use of filters (RFC4661 [128], rate control [113] and loc-filters [129]) may be used to control notification.

An element needing location that has a HELD URI must dereference per draft-winterbottom-geopriv-deref-protocol [78].

[14] A LIS, if it implementes 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.

An access network that provides location by reference must supply either a SIP or a HELD location reference URI per Section 4.2. Networks that use other protocols must interwork to SIP or HELD. Elements in the ESInet which receive a location reference and forward location in SIP signaling to another element must pass the reference, and not any value it determines 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.

The LIS must accept the ESRP and PSAP credentials traceable to the PSAP Credentialing Agency (PCA) to deliver location with the required confidence/uncertainty.

Other than the above, the implementation used within the origination and access networks for support of location is out of scope of this document.

5.3 Provisioning

The user account provisioning mechanism used in this specification is based on System for Cross-domain Identity Management (SCIM) [91]. Further details will be provided in a future version.

5.4 Policy

Policy is stored into and retrieved from the Policy Store using a web service. This section describes the "Policy Store Web Service" in Section 4.4.1 that allows to upload and to retrieve 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 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 us 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 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.

5.4.1 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 the first chunk of the policy set if it is large, plus an identifier that can be used with MoreRetrievePolicy to obtain more chunks of a large policy set if the policy is too large to send in the response, and an expiration time. The policy store may reduce the size of the chunk returned if it us 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	Optional	Id to be used with MoreRetrievePolicy. Must be present if policyDataChunk is returned, but is not the complete policy

Referral	Optional	URI of another policy store that may have this policy.
errorCode	Optional	Error Code if no policy or referral is returned

Error Codes

100	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
errorCode	Optional	Error Code if no policy or referral is returned

Error Codes

100	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 request.
nextChunkId	Optional	Id to be used with MoreStorePolicy.
errorCode	Optional	Error Code

Error Codes

100	Okay No error (optional to return)
501	Unknown or bad Policy Name
502	Unknown or bad Agency Name
504	Unspecified Error
506	Policy Too Large
507	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	Optional	Id to be used with MoreRetrievePolicy if not the last chunk
errorCode	Optional	Error Code if no policy or referral is returned

Error Codes

100	Okay No error (optional to return)
504	Unspecified Error
505	Bad chunkId
508	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
errorCode	Optional	Error Code if no policy

Error Codes

100	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 UpdatedPolicy 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
errorCode	Optional	Error Code if no policy

Error Codes

100	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).

5.4.2 Policy Syntax

This section summarizes the syntax and semantic of the policy language used for making call routing decisions. Policy is represented in an RFC4745 [147] 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 RFC4745, this document is composed of rules that contain three parts - conditions, actions, and transformations. The condition statement may either evaluate to 'true' or 'false'. If it evaluates to 'true' then the action, and the transformation part of the rule is executed. In order to deal with the case where multiple condition parts evaluate to 'true' a conflict resolution mechanism is described to avoid conflicting actions to be executed. Common Policy described a conflict resolution and this document extends Common Policy with a priority based mechanism whereby each rules has a priority value associated 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.

5.4.2.1 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.

5.4.2.1.1 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 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 TIME data type as mentioned in Section 4.3.12 of RFC 2445. Time is local time at the PSAP, including daylight savings. This attribute is optional. The default value is 000000.

timeend: End of time interval in a particular day. It is of the TIME data type as mentioned in Section 4.3.12 of RFC 2445. Time is local time at the PSAP, including daylight savings. This attribute is optional. The default value is 235959.

byweekday: List of days of the week. This attribute is optional.

The <time-period> is based on the description in CPL but with a reduced feature set.

The "dtstart" and "dtend" attributes are formatted as timestamps.

The "timestart" specifies a time value to indicate the beginning of every day. The default value is 000000 representing the beginning of the day.

The "timeend" specifies a time value to indicate the end of every day. The default value is 235959 representing the end of the day.

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.

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 'dtstart' is long enough to accommodate the specified values, else they are just neglected.
3. If the values of the 'byweekday' attribute values do not correspond to the expected domain, they are simply ignored.
4. Only a single 'byweekday' attribute MUST be listed in a <time> element.

5.4.2.1.2SIPHeader 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>. Currently, only a single operator is defined, namely an equality match. The defined value is "equal" in the <operator> element.

The semantic of this field is to compare the content of a specific header field with a pre-defined content.

5.4.2.1.3MIME 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.

5.4.2.1.4Location Conditions

This document re-uses the location-based condition elements from ietf-geopriv-policy [146].

5.4.2.1.5Call 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".

5.4.2.1.6SecurityPosture 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.

5.4.2.1.7QueueState 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

5.4.2.2 Actions

As stated in [RFC4474], conditions are the 'if'-part of rules, whereas actions and transformations form their '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.

5.4.2.2.1Priority

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.

5.4.2.2.2Route 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 <causes>, 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 <causes> contains the value used with the Reason header associated with a History-Info header. The <recipient> element is mandatory, and the <causes> element is optional.

5.4.2.3 LoSTServiceURN Action

The <LoSTServiceURN> element carries the Service URN (urn:service:...) as the value. The resulting URI is a variable called "NormalNextHop", available to the rule evaluation system.

5.4.2.3.1Busy Action

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

5.4.2.3.2Notify 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.

5.4.2.4 Namespace

This document uses the European Emergency Services URN namespace "urn:EES:policy-v1".

5.5 LoST

LoST is the protocol that is used for two functions: call routing and location validation.

- Call routing: LoST is used by the ECRF as the protocol to route all emergency calls both to[15] and within the ESInet.
- Location validation: LoST is used by the LVF as the protocol to validate location information for every call origination end device prior to any potential use for emergency call routing.

Each LoST message is an XML-based document. The root element within each LoST message has the same name as the LoST message name and contains attributes and other elements. In Section 4.5.1 and its sub-sections, XML attributes are denoted by "attributeName" and XML elements by "<elementName>" (e.g., sourceId and <displayName>).

In the following sections, there is text that explains how LoST works. The normative reference that defines the protocol is RFC5222 [61].

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[16] 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 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 address for 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.

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 NG112, the URI returned may not be that of a PSAP, but instead may route to an ESRP.

[15] 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 calls are routed to the same ESRP as would the use of LoST to the ECRF.

[16] 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.

5.5.1.1 LoST Call Routing Messages

The LoST interface message used to query for the next hop within the ESInet is the <findService> message. The LoST interface message used to return the result of processing a <findService> request message is the <findServiceResponse> message. The ECRF receiving the <findService> message translates the Service URN and location information in the message into a next-hop URI, which is returned in the <findServiceResponse> message to the querying entity. If the ECRF cannot successfully process a <findService> message, it returns an <error> message. The following three sections describe these messages.

5.5.1.1.1LoST <findService> Request Message

A querying entity (e.g., ESRP, VoIP-based endpoint, Legacy Network Gateway, Legacy PSAP Gateway, PSAP) uses the <findService> message to retrieve one or more contact URIs from an ECRF given a Service URN and a location. This message contains elements and attributes specified in Table 5-1. Note the "Name" column contains the actual <findService> message's attribute and element names as defined by the LoST protocol.

Table 5-1 – LoST <findService> Message Attributes and Elements

Name	Condition	Purpose
Xmlns	Mandatory	This attribute specifies the LoST protocol's XML namespace.
<location>	Mandatory	This element contains either civic address- or geodetic coordinates-based location information.
Recursive	Optional	This attribute indicates a preference for a recursive or iterative query.
<service>	Mandatory	This element contains the URN of the requested service.
<path>	Conditional	This element indicates the path the message has taken through ESRPs within the ESInet.
serviceBoundary	Optional	This attribute indicates how the service boundary should be returned to the requestor.
validateLocation	Conditional	This attribute indicates whether the civic address location should be validated.

The LoST <findService> message attributes and elements specified in Table 5-1 are described in greater detail below.

- xmlns Attribute

  This required attribute must specify the LoST protocol XML namespace and is coded as follows.

xmlns="urn:ietf:params:xml:ns:lost1"

- <location> Element

  This required element carries the location information used to query for routing information and has the format specified in [61]. The location information can be in the form of a civic address or geodetic coordinates. The civic address-based location information format is specified in RF4119 [6] updated by RFC5139 [76] and RFC5491 [75]. The geodetic coordinates-based location information format is specified in [75] and the supported geographic shapes are point, polygon, circle, ellipse, and arc band. See Section 8.2 in [61] for examples of civic and geodetic-2d location information encodings.

  There must be one and only one <location> element. Although the LoST protocol permits multiple <location> elements with one per unique location profile based on the same baseline location profile in a single LoST <findService> message, this document limits the number of <location> elements to exactly one. For maximum client/server interoperability, there should be only one <location> element based on a baseline location profile in a <findService> message sent to an ECRF. See Section 12 in [61] for more information about baseline and derived location profiles.

  The "location" element contains many elements and attributes, some of which are described in Table 5-2.

- recursive Attribute

  LoST servers can operate in recursive mode or iterative mode if a mapping is not found based on the coding of this attribute.

  - The use of recursion by the ECRF initiates a query on behalf of the requestor that propagates through other ECRFs to an authoritative ECRF that returns the PSAP URI back through the intervening ECRFs to the requesting ECRF.

  - The use of iteration by the ECRF simply returns a domain name of the next ECRF to contact.

  This optional attribute is coded “true” to indicate recursive mode or “false” or not coded to indicate iterative mode.

  The ECRF may operate in a recursive mode or an iterative mode, depending on local implementation.

- <service> Element

  This required element identifies the service requested by the client. Valid service names are specified in [58] and must be "sos" or one of its sub-services for ECRFs and LVFs used by originating networks or devices. For internal ECRFs used by entities within the ESInet to route calls, the <service> element may be a service URN beginning “urn:ees”.

- <path> Element

  This conditional element contains <via> elements indicating the ECRFs (LoST servers) that have handled the <findService> request as a recursive query. This element is used by ECRFs to detect a recursive query routing "loop" during recursive query processing. See Section 6 in [61] for detailed information about the <path> element.

  The order of <via> elements within the <path> element is significant. The first <via> element always indicates the ECRF that received the initial <findService> message query from the requesting ESRP. The last <via> element indicates the ECRF that sent the <findService> request to the current ECRF. All <via> elements indicate the path from the initiating ECRF to the current ECRF.

  The originating ESRP that sends the <findService> message to the initial ECRF does not include this element in the message; i.e., it is an error for the <path> element to exist within the <findService> message sent by any element except an ECRF.

  When an ECRF receives a <findService> message, it appends its own domain name as a new last <via> element to the <path> element before forwarding the <findService> message to another ECRF or returning a <findServiceResponse> message (which contains the <path> element).

- serviceBoundary Attribute

  A requesting entity can obtain the boundary of the jurisdiction or service area handled by the requested service. This is most useful for mobile devices that use geodetic coordinates since they can track their location. When they leave the jurisdictional area, they can send another <findService> request to determine the proper jurisdiction for their new location.

  This optional attribute indicates whether a service boundary value or reference is preferred in the <findServiceResponse> message. The query originator can express a preference for a value or a reference using this attribute, but the ECRF makes the final decision as to whether to return a reference, a value, or even nothing.

  This attribute is coded "value" to indicate the preference for returning the service boundary as a value or is omitted or coded "reference" to indicate the preference for returning the service boundary as a reference. The <serviceBoundary> element returns the service boundary "value" and the <serviceBoundaryReference> element returns the "reference".

  Note that returning the service boundary as a reference passes less data in a message, using less network bandwidth, but requires later dereferencing via a LoST <getServiceBoundary> message to obtain the value, thus later using more server time and increasing call delay. Returning the service boundary as a value passes more data in a message, using more network bandwidth, but does not require later dereferencing, thus saving server time and minimizing call delay. In addition, a service boundary may require many data points to accurately identify the boundary of a jurisdiction or service area, possibly making the service boundary dataset very large.

According to [61], a LoST server may decide, based on local policy, to return the service boundary as a value or a reference, or even not to return the service boundary information by omitting both the <serviceBoundary> and <serviceBoundaryReference> elements in the <findServiceResponse> message. This means the requesting entity must handle a returned value, a returned reference, or nothing regardless of the "value" or "reference" coding or the omission of the serviceBoundary attribute in the <findService> message. ECRFs should return a service boundary if the request included the attribute.

- validateLocation Attribute

  Location validation is the validation of civic address-based location information against an authoritative GIS database containing only valid civic addresses obtained from 112 Authorities.

  Location validation is performed by the LVF. Normally, an i3 ECRF does not perform location validation because this architecture requires location information to be validated before it is passed in SIP call signaling to an ESRP; hence, an ESRP will not normally request location validation of an ECRF.

  This optional attribute 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 RFC5222. This may be changed in a future edition to allow validation of a geodetic location.

  The validateLocation attribute is coded "true" to request location validation or is omitted or coded "false" to request no location validation. For i3 emergency call routing, this attribute normally will be omitted.

The attributes and elements of the <location> element given in Table 5-1 above are specified in Table 5-2 below along with a short description of their purpose. Note only the two-dimensional (2D) geoshapes—Point, Polygon, Circle, Ellipse, and Arcband, are supported for geodetic coordinates-based locations.

Table 5-2 – LoST <location> Element Attributes and Elements

Name	Condition	Purpose
Profile	Mandatory	This attribute defines the profile of the location information; i.e., the nature of the location information (civic or geodetic).

Name	Condition	Purpose
Id	Mandatory	This attribute defines an id uniquely identifying the <location> element within the <findService> message.
Xmlns	Conditional	This attribute specifies an XML namespace appropriate to the location profile.
<Point>	Conditional	This element defines a "point" geodetic shape-based location.
<Polygon>	Conditional	This element defines a "polygon" geodetic shape-based location.
<Circle>	Conditional	This element defines a "circle" geodetic shape-based location.
<Ellipse>	Conditional	This element defines an "ellipse" geodetic shape-based location.
<Arcband>	Conditional	This element defines an "arcband" geodetic shape-based location.
<civicAddress>	Conditional	This element defines a civic address-based location.

The LoST <location> element attributes and elements specified in above are described in greater detail below.

- profile Attribute

  This required attribute specifies the nature of the location information contained within the <location> element and, therefore, how the information is encoded and should be interpreted.

  This attribute is coded "civic" for a civic address-based location profile and "geodetic-2d" for a geodetic coordinates, shape-based location profile.

  The "civic" and "geodetic-2d" profiles are baseline profiles defined by section 12 in [61]. In order to obtain maximum interoperability for emergency call routing, the ESRP and ECRF should use only "baseline" profiles for location information encoding**.**

- id Attribute

  This required attribute uniquely identifies its <location> element within the <findService> message. If multiple <location> elements were to be present within the message, this attribute must have a unique value for each <location> element. However, the query is limited to only have one <location> element.

When the ECRF determines a route, it indicates which <location> element was successfully used to determine the route by copying the value of this attribute to the id attribute of the <locationUsed> element in the <findServiceResponse> message; thus permitting the requesting entity to identify the <location> element successfully used by the ECRF.

This attribute can be coded with any value. Since LoST permits only profiles based on a single baseline profile in a <findService> request and only baseline profiles in the request are permited, there will be only one <location> element, which makes this attribute somewhat superfluous. Notwithstanding, LoST requires it.

- xmlns Attribute

This attribute specifies an XML namespace that defines the markup language for the specified location profile. It will specify the PIDF-LO civic address XML namespace that defines the elements and their attributes for civic address-based location information, or the PIDF-LO geodetic shapes XML namespace that defines the elements (described below) and their attributes used for geodetic coordinates-based location information.

When the profile attribute is coded "civic", this attribute must be coded for the PIDF-LO civic address (see [76]) namespace. For example:

xmlns:ca="urn:ietf:params:xml:ns:pidf:geopriv10:civicAddr"

When the profile attribute is coded "geodetic-2d", this required attribute must be multiply-coded with the namespaces for generic GML shapes and specific PIDF-LO geodetic shapes (see sections 4 and 5 of [75] and [100]). The geoShapes namespace defines a subset of the GML namespace shapes in a manner appropriate to PIDF-LO, but does not redefine all shapes or attributes; hence the need to reference the GML namespace as well.

The example below shows XML namespace prefixes of "gml" and "gs". Since both namespaces define mutually named shapes, the appropriate geographic and geoshape element names would be qualified with the appropriate prefixes (e.g., <gml:Point> and <gml:pos>).

xmlns:gml="http://www.opengis.net/gml"

xmlns:gs="http://www.opengis.net/pidflo/1.0” "

Typically, the xmlns would not appear in the <location> element, but rather would appear in the location profile element (e.g., <civic address>). If an xmlns for a location profile is found in the <location> element, it must declare a prefix.

- <Point> Element

This conditional element specifies point shape-based, geodetic coordinates location information (e.g., <gml:Point>). Use of this element is described in section 12.2 of [61] and the element is described in section 5.2.1 of [75] and in [100]. <Point> is part of the http://www.opengis.net/gml namespace.

This attribute is conditioned on the profile attribute coded "geodetic-2d"; i.e., it is an error to specify this element when the profile attribute is not coded "geodetic-2d".

- <Polygon> Element

  This conditional element specifies polygon shape-based, geodetic coordinates location information (e.g., <gml:Polygon>). Use of this element is described in section 12.2 of [61] and the element is described in section 5.2.2 of [75] and in [100]. <Polygon> is part of the http://www.opengis.net/gml namespace.

  This attribute is conditioned on the profile attribute coded "geodetic-2d"; i.e., it is an error to specify this element when the profile attribute is not coded "geodetic-2d".

- <Circle> Element

  This conditional element specifies circle shape-based, geodetic coordinates location information (e.g., <gs:Circle>). Use of this element is described in section 12.2 of [61] and the element is described in section 5.2.3 of [75] and in [100]. <Circle> is part of the http://www.opengis.net/pidflo/1.0 namespace

  This attribute is conditioned on the profile attribute coded "geodetic-2d"; i.e., it is an error to specify this element when the profile attribute is not coded "geodetic-2d".

- <Ellipse> Element

  This conditional element specifies ellipse shape-based, geodetic coordinates location information (e.g., <gs:Ellipse>). Use of this element is described in section 12.2 of [61] and the element is described in section 5.2.4 of [75] and in [100]. <Ellipse> is part of the http://www.opengis.net/pidflo/1.0 namespace

  This attribute is conditioned on the profile attribute coded "geodetic-2d"; i.e., it is an error to specify this element when the profile attribute is not coded "geodetic-2d".

- <Arcband> Element

  This conditional element specifies arcband shape-based, geodetic coordinates location information (e.g., <gs:Arcband>). Use of this element is described in Section 12.2 of [61] and the element is described in Section 5.2.5 of [75] and in [100]. <Arcband> is part of the http://www.opengis.net/pidflo/1.0 namespace.

This attribute is conditioned on the profile attribute coded "geodetic-2d"; i.e., it is an error to specify this element when the profile attribute is not coded "geodetic-2d".

- <civicAddress> Element

  This conditional element specifies civic address-based location information. Section 12.3 of [61] describes use of this element and [6] and [76] describe the element and its attributes. <civicAddress> is part of the urn:ietf:params:xml:ns:pidf:geopriv10:civicAddr namespace.

  Table 5-3 gives a short description of many child elements used to specify civic address information. Note that the LoST request does not include a PIDF-LO, but rather has some of the same elements as the PIDF-LO. The requestor copies those elements from the PIDF-LO to the LoST request.

  This attribute is conditioned on the profile attribute coded "civic"; i.e., it is an error to specify this element when the profile attribute is not coded "civic".

Table 5-3 PIDF <civicAddress> Element Attributes and Elements

Name	**Description**	**Example**
<country>	2-letter ISO code	US
<A1>	national subdivision (e.g., state)	NY
<A2>	county, parish	King's County
<A3>	city, township	New York
<A4>	city division, borough	Manhattan
<A5>	neighborhood	Morningside Heights
<A6>[17]	street name (deprecated)	
<RD>	primary road name	Broadway
<PRD>	leading street direction	N

[17] RD must be used instead of A6. ESInet elements should accept A6 and treat as RD. If both are present and they are not the same value, it should be treated as an error.

Name	Description	Example
<POD>	trailing street suffix	SW
<STS>	street suffix	Ave
<HNO>	house number	123
<HNS>	house number suffix	A, 1/2
<LMK>	Landmark or vanity address	Columbia University
<LOC>	additional location info	South Wing
<NAM>	name (residence or office occupant)	Town Barber Shop
<PC>	postal or ZIP code	10027-0401
<BLD>	building (structure)	Low Library
<UNIT>	unit (apartment, suite)	Apt 42
<FLR>	floor	4
<ROOM>	room	450F
<PLC>	type of place	office
<PCN>	postal community name	Leonia
<ADDCODE>	additional code	132030000003
<SEAT>	Seat (desk, workstation, cubicle)	WS 181
<RDSEC>	road section	14
<RDBR>	branch road name	Lane 7
<RDSUBBR>	sub-branch road name	Alley 8
<PRM>	Road name pre-modifier	Old
<POM>	Road name post-modifier	Service

5.5.1.1.2LoST <findServiceResponse> Message

When the ECRF successfully processes a LoST <findService> message, it returns a LoST <findServiceResponse> message containing the "next hop" ESRP or final PSAP URI. If the ECRF cannot successfully process a LoST <findService> message, it returns a LoST <errors> message indicating the nature of the error (see section 5.5.1.1.3) or a LoST <redirect> message indicating the ECRF that can process the

<findService> message (see section 5.5.1.1.4). Table 5-4 specifies the elements and attributes of the <findServiceResponse> message.

Table 5-4 – LoST <findServiceResponse> Message Attributes and Elements

Name	Condition	Purpose
xmlns	Mandatory	This attribute specifies the LoST protocol's XML namespace.
<path>	Mandatory	This element indicates the ECRF(s) (LoST servers) that handled the request.
<locationUsed>	Optional	This element identifies the location used by the ECRF to determine the service URI.
<mapping>	Mandatory	This element identifies a service region and its associated service URIs.

The elements and attributes that make up the <findServiceResponse> message are described below:

- xmlns Attribute

  This required attribute specifies the LoST protocol XML namespace and should be coded as specified by section 17.4 in [61] (shown below).

  xmlns="urn:ietf:params:xml:ns:lost1"

- path

  This element contains <via> elements indicating the ECRF(s) that handled the <findService> request. See section 6 in [61] for detailed information about the <path> element.

  The order of <via> elements within the "path" element is significant. The first <via> element always indicates the ECRF (LoST server) that received the initial <findService> message query from the requesting entity.

  For a recursive query, the last <via> element indicates the authoritative ECRF and any intervening <via> elements between the first and last <via> elements indicate the path from the initiating ECRF to the authoritative ECRF.

  For an iterative query, there are <via> elements indicating the ECRFs that were contacted during processing of the <findService> request.

- locationUsed

  This optional element identifies the <location> element within the <findService> message used to successfully determine the service URI.

  The value of this element is a copy of the value from the id attribute of the <location> element successfully processed by the ECRF.

- mapping

  This required element returns the service information to the requesting entity when the ECRF successfully processed the <findService> message.

  The "mapping" element contains many elements and attributes described in Table 5-5

Table 5-5 LoST <mapping> Element Attributes and Elements

Element/Attribute	Condition	Purpose
source	Mandatory	Identifies the authoritative generator of the mapping
sourceId	Mandatory	Identifies a particular mapping
lastUpdated	Mandatory	Describes when a mapping identified by the source and sourceId was last updated
expires	Mandatory	Identifies the absolute time when the mapping becomes invalid
displayName	Optional	Describes a human readable display name, e.g., the name of the PSAP serving the location (may be repeated)
service	Mandatory	Identifies the service for which the mapping applies
serviceBoundary	Optional	Identifies the area where the URI returned would be valid
serviceBoundaryReference	Optional	Identifies the reference that can be used to access the service boundary for which the URI returned is valid

Element/Attribute	Condition	Purpose
serviceNumber	Optional	Provides the emergency services dial string that is appropriate for the location provided in the query
uri	Conditional[18]	Contains the appropriate contact URI for the requested service. May be repeated when multiple protocols are accepted at the destination. Not intended to support multiple destinations.
locationValidation	Optional	Indicates which elements of the civic location were "valid" and used for mapping, which elements were "invalid" and which elements were "unchecked"

The attributes and elements that make up the LoST "mapping" element specified in Table 5-5 above are described below:

- source Attribute

  This element identifies the authoritative generator of the mapping (the LoST server that generated the mapping). LoST servers are identified by U-NAPTR/DDDS application unique strings, in the form of DNS name (e.g., lostserver.notreal.com).

- sourceId Attribute

  This element identifies a particular mapping at the LoST server and is unique among all the mappings maintained by the LoST server.

- lastUpdated Attribute

  This element describes the date and time when this specific instance of mapping was updated. The date and time is represented in UTC format.

- expires Attribute

  This element describes the date and time when a particular mapping becomes obsolete. The date and time are described using a timezoned XML type datetime. This element may optionally contain the values of "NO-CACHE" indicating that the mapping should not be cached and "NO-EXPIRATION" indicating that the mapping has no expiration instead of the date and time.

[18] The ECRF includes one or more URIs in a <findServiceResponse> message if one can be determined. Absence of a URI indicates a mapping exists, but no URI is provided in that mapping. This should not occur.

- <displayName> Element

  The display name 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.

- <service>

  The <service> element identifies the service for which this mapping is valid. The ECRF is required to support the "sos" service. Support for other services will depend on local implementation.

- <serviceBoundary>

  The <serviceBoundary> element identifies the geographical area where the returned mapping is valid. The intent of this parameter is to allow a mobile endpoint to realize that it is moved out of the area where a stored mapping is valid and trigger it to query for a new valid mapping. This element may be supported by the ECRF depending on local implementation.

- <serviceBoundaryReference>

  The <serviceBoundaryReference> element identifies a reference that could be used to access the service boundary for the requested mapping. This parameter may be supported by the ECRF depending on local implementation.

- <serviceNumber>

  The <serviceNumber> element 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.

- Uniform Resource Identifier (<uri>)

  The URI specifies either the address of the PSAP or the ESRP that is appropriate for the location sent in the query message. The decision of whether to send the PSAP URI or the ESRP URI is based on

  a) whether the query is made by the end user, VSP Routing Proxy, PSAP, or the ESRP (which would be determined by the credentials presented in the establishment of a TLS connection to the ECRF) and/or
  b) the service urn presented in the query.

- <locationValidation>

  The <locationValidation> element identifies which elements of the received civic address were "valid" and used for mapping, which were "invalid" and which were unchecked. Since the ECRF is not responsible for performing validation, this parameter may not be returned, subject to local implementations.

5.5.1.1.3LoST <errors> Message

If the ECRF cannot successfully process a <findService> message, it returns the <errors> message instead of the <findServiceResponse> message. The <errors> message contains information indicating the nature and source of the error.

Table 5-6 – LoST <errors> Message Attributes and Elements

Name	Condition	Purpose
xmlns	Mandatory	This attribute specifies the LoST protocol's XML namespace.
source	Mandatory	This attribute specifies the source of the error.
<badRequest> <forbidden> <internalError> <locationProfileUnrecognized> <locationInvalid> <SRSInvalid> <loop> <notFound> <serverError> <serverTimeout> <serviceNotImplemented>	Mandatory	These elements specify error types.

The LoST <errors> message attributes and elements specified in Table 5-6 are described in greater detail below.

- xmlns Attribute

  This required attribute must specify the LoST protocol XML namespace and is coded as follows.

  xmlns="urn:ietf:params:xml:ns:lost1"

- source Attribute

  This required attribute identifies the source of the error, which will be in the form of a DNS name (e.g., ecrf.example.com).

The following LoST <errors> message child elements describe the types of errors encountered or detected by the ECRF. They give the requesting entity a limited set of "error types", each of which is likely to be handled in a particular manner by the requesting entity regardless of the nature of the actual error (see message attribute below). One or more "error type" elements can be returned in the <errors> message. See section 13.1 of [61] for an explanation of each error type.

- <badRequest> Element

  This element indicates the ECRF 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 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 could not satisfy a request due to a bad configuration or some other operational and non-LoST protocol-related reason.

- <locationProfileUnrecognized> Element

  This element indicates the ECRF did not recognize the value of the profile attribute sent with the <findService> request; i.e., it was not coded with "civic" or "geodetic-2d".

- <locationInvalid> Element

  This element indicates the ECRF determined the geodetic or civic location is invalid (e.g., geodetic latitude or longitude value is outside the acceptable range).

- <SRSInvalid> Element

  This element indicates the ECRF 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., profile="geodetic-2d" and <civicAddress> element present).

- <loop> Element

  This element indicates an ECRF detected a loop during a recursive query; i.e., an ECRF finds the "next hop" URL is already in a <via> element within the <path> element of the <findService> request.

- <notFound> Element

  This element indicates the ECRF could not find an answer to the query.

- <serverError> Element

  This element indicates the ECRF received a response from another ECRF for a recursive query but could not parse or understand the response.

- <serverTimeout> Element

  This element indicates the ECRF timed out waiting for a response (e.g., another ECRF for a recursive query, the SIF server, etc.).

- <serviceNotImplemented> Element

  This element indicates the ECRF detected the requested service URN is not implemented and it found no substitute for it.

Each of the preceding "error type" elements can have the following attributes.

Table 5-7 – LoST "Error Type" Element Attributes

Name	Condition	Purpose
message	Optional	This attribute specifies additional human-readable information about an error.
xml:lang	Conditional	This attribute specifies the language in which the message attribute's value is written.

The LoST <errors> message "error type" element's attributes specified in Table 5-7 are described in greater detail below.

- message Attribute

  This optional attribute specifies human-readable text indicating a more particular or specific reason for the error (e.g., message="LoST server encountered a software bug.").

- xml:lang Attribute

  This conditional attribute specifies the language in which the message text is written (e.g., xml:lang="en" indicates English). This attribute is conditioned on the message attribute; i.e., this attribute should not be present if the message attribute is not present. Further, if the message attribute is present, this attribute should be present so the text of a message can be properly displayed, logged and/or interpreted.

5.5.1.1.4LoST <redirect> Message

If the ECRF cannot or should not handle a <findService> message for any reason (e.g., failover, etc.) but does know the ECRF that can, it returns the <redirect> message to the requesting entity instead of the <findServiceResponse> or <errors> message. This message returns information indicating the source of and reason for the redirection and the URL of the ECRF to which the requesting entity should redirect its <findService> message.

Table 5-8 – LoST <redirect> Message Attributes and Elements

Name	Condition	Purpose
xmlns	Mandatory	This attribute specifies the LoST protocol's XML namespace.
target	Mandatory	This attribute specifies the target of the redirection.

Name	Condition	Purpose
source	Mandatory	This attribute specifies the source of the redirection.
message	Optional	This attribute specifies additional human-readable information about the redirection.
xml:lang	Conditional	This attribute specifies the language in which the message attribute's value is written.

The LoST <redirect> message attributes and elements specified in Table 5-8 are described in greater detail below.

- xmlns Attribute

  This required attribute must specify the LoST protocol XML namespace and is coded as follows.

  xmlns="urn:ietf:params:xml:ns:lost1"

- target Attribute

  This required attribute identifies the target of the redirection, i.e., the domain name of the ECRF to which the requesting entity should send its <findService> message.

- source Attribute

  This required attribute identifies the source of the redirection, which will be in the form of a DNS name (e.g., ecrf.example.com).

- message Attribute

  This optional attribute specifies human-readable text indicating a more particular or specific reason for the redirection (e.g., message="LoST server has temporarily failed over to another system.").

- xml:lang Attribute

  This conditional attribute specifies the language in which the message text is written (e.g., xml:lang="en" indicates English). This attribute is conditioned on the message attribute; i.e., this attribute should not be present if the message attribute is not present. Further, if the message attribute is present, this attribute should be present so the text of a message can be properly displayed, logged and/or interpreted.

5.5.1.1.5LoST Common XML Namespaces Summary

All LoST messages have root and other elements that require specification of XML namespaces for their proper interpretation. Table 5-9 shows LoST elements that require specification of the xmlns attribute to define their appropriate XML namespace. Some elements may require more than one xmlns attribute since their sub-elements contain elements defined by more than one namespace.

Table 5-9 – LoST Protocol Message Elements and xmlns Attribute Common Namespaces

Name	xmlns Attribute Value	Defines
<findService> <findServiceResponse> <errors> <redirect>	urn:ietf:params:xml:ns:lost1	LoST protocol elements
<location>	urn:ietf:params:xml:ns:lost1 urn:ietf:params:xml:ns:pidf:geopriv10:civicAddr http://www.opengis.net/pidflo/1.0 http://www.opengis.net/gml	LoST protocol elements Civic address elements Geoshape elements GML elements
<serviceBoundary>	urn:ietf:params:xml:ns:lost1 urn:ietf:params:xml:ns:pidf:geopriv10:civicAddr http://www.opengis.net/pidflo/1.0 http://www.opengis.net/gml	LoST protocol elements Civic address elements Geoshape elements GML elements

5.5.1.1.6LoST srsName Attribute Common URNs Summary

GML and geoshape elements require an srsName attribute to specify a URN that defines their interpretation. Table 5-10 shows GML and geoShape elements that require specification of the srsName attribute and their possible URN value(s). Some elements may require more than one srsName attribute since their child elements contain elements defined by more than one URN.

Table 5-10 - GML and geoShape Elements and srsName Attribute Common URNs

Name	srsName Attribute Value	Defines
<gs:Point> <gs:Polygon> <gs:Circle> <gs:Ellipse> <gs:Arcband>	urn:ogc:def:crs:EPSG::4326	Two-dimensional (2D) shapes
<gs:height>	urn:ogc:def:uom:EPSG::9001	Distance Unit of Measure in meters
	urn:ogc:def:uom:EPSG::9101	Angular Unit of Measure in radians
	urn:ogc:def:uom:EPSG::9102	Angular Unit of Measure in degrees
<gml:pos>		Latitude and Longitude in decimal degrees

5.5.1.2 Call Routing Scenarios

The following examples are preliminary. Further examples will be provided in a future edition of this document

5.5.1.2.1Civic Address-based Call Routing LoST Interface Example Scenario

```
<?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>DR</STS>
```

```
   <HNO>2901</HNO>
      <NAM>Courtyard Marriott</NAM>
      <RM>Board Room B</RM>
   <PC>43219</PC>
  </civicAddress>
 </location>
 <service>urn:service:sos</service>
</findService>
```

A <findService> well-formed civic address 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"/>
     <locationUsed id="627b8bf819d0bcd4d"/>
   </findServiceResponse>
```

A <findServiceResponse> Response to Well-formed 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>
         <A3>Columbus</A3>
         <RD>Airport</RD>
              <STS>DR</STS>
         <HNO>2901</HNO>
         </civicAddress>
     </location>
     <service>urn:service:sos</service>
   </findService>
```

A <findService> civic address query with partial info

```
<?xml version="1.0" encoding="UTF-8"?>
   <errors xmlns="urn:ietf:params:xml:ns:lost1"
     source="ecrf.state.oh.us">
      <internalError message="notFound" xml:lang="en"/>
   </errors>
```

A <error> Response to partial-formed query

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

5.5.1.2.2Geodetic Coordinates-based Call Routing LoST Interface Scenario

To be provided in a future edition of this document

5.5.2 Location Validation

"Validating" a location in NG112 means querying the Location Validation Function (Section 4.5) to determine if the location is suitable for use (specifically, if the location can be used to accurately route the call and dispatch responders). The LVF uses the same LoST interface as routing as defined above, with the validateLocation option in the <findservice> request set to true.

5.5.3 LoST Mapping Architecture

So far, we have described the LoST protocol as it is described in RFC 5222 [140], namely as a client-server protocol. A single LoST server, however, does not store the mapping elements for all PSAPs worldwide, for both technical and administrative reasons. Thus, there is a need to let LoST servers interact with other LoST servers, each covering a specific geographical region. The LoST protocol already provides the baseline mechanisms for supporting such a communication architecture, as described in RFC 5582 [227], an informational writeup providing terminology (in the form of different roles for LoST servers that distinguish their behavior) and explaining the basic concept of the LoST mapping architecture. RFC 5582 motivates the basic design decision for LoST to utilize it in a wide variety of architectures but leaves the detailed instantiation to deployments in different jurisdictions.

The awareness of peering LoST servers determines the structure of the architecture rather than certain physical properties of a network, such as topology of a fibre installation, or the structure of a national emergency services organization. Two types of structures used in combination, namely a mesh and a hierarchical structure. The mesh topology is envisioned for the top-level LoST entities whereas the hierarchical structure reflects a parent - child relationship in a tree. Figure 2 shows this structure graphically with the LoST servers acting in their roles of forest guides (FGs), and trees. A tree consists of a self-contained hierarchy of authoritative mapping servers (AMS) for a particular service.

An AMS is a LoST server that can provide the authoritative answer to a particular set of queries. The top-most server in a tree is a tree root and this server peers with one or multiple FGs, i.e., the tree root announces its coverage region to FGs.

In Figure 2, for example, the root of tree 1 interacts with FG A and makes the coverage area available. FG A also receives the coverage area from the root of tree 2. All tree roots receive themselves information about the coverage area of their children in the tree. On the top level all FGs (namely FG A, FG B, and FG C) form a mesh and synchronize their coverage areas. Seekers, and resolvers are two additional LoST entities in the LoST mapping architecture that are not shown in Figure 2. Neither seekers nor resolvers provide authoritative answers themselves but they may cache results. Particularly the usage of resolvers to cache mapping elements is expected to be very common.

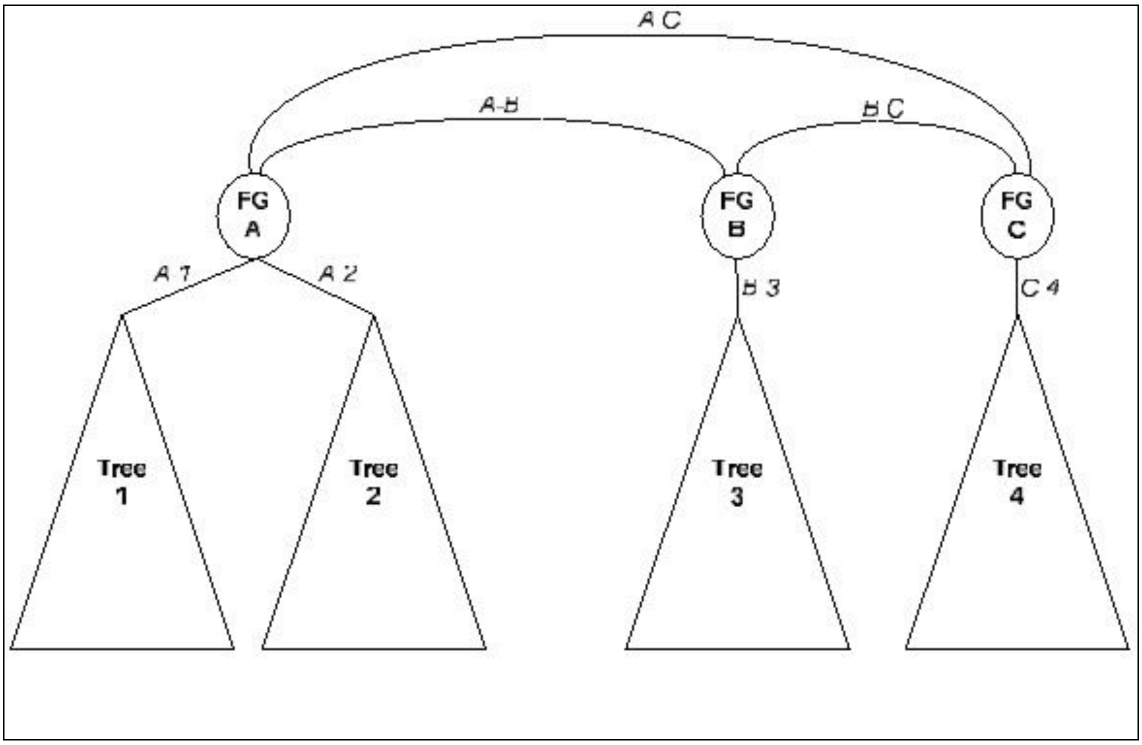


Figure 2: Trees and Forest Guides in the LoST Mapping Architecture.

To best understand the LoST mapping architecture it is important to highlight the main design goals:

- **Robustness:** To ensure the stability of the system even if different people in different places of the LoST architecture make different decisions the system will still function. It cannot be assumed that everyone has to agree with everyone else. The minimum level of agreement that has to be ensured is that AMSs are able to authoritatively answer mapping queries, i.e., only those LoST servers respond authoritatively if they indeed have the authority of a specific coverage area.
- **Consistent Responses:** Any device (called seeker) can issue a LoST query and it will get a consistent answer regardless of where the query enters the

system. In some (rare) cases of territorial disputes, two AMSs may claim authoritative for the same region. In such a case the answer received by a seeker will vary depending on the entry point into the mapping system.

- **Scalability:** Scalability of the LoST architecture is ensured by the usage of caching and the distributed nature of the LoST servers in the architecture. Any LoST entity may support caching of received mapping elements. The mapping elements may be obtained as part of the ordinary operation of LoST (via query and responses) but also via separate replication of the mapping elements. LoST Sync [235] is one such protocol to exchange mappings between LoST servers. This specification also describes an additional approach.
- **Minimal Seeker Configuration:** A seeker is a LoST client requesting a mapping. The only information a seeker needs to know is the address of a resolved; it does not need to know the structure of all Forest Guides nor or does it need to maintain a global picture of LoST servers. To avoid having end user involvement in the configuration of LoST servers, Section 4 of the LoST specification provides a discovery technique based on DNS and RFC 5223 [233] offers a DHCP-based discovery procedure. Although LoST servers can be located anywhere, a placement topologically closer to the end host, e.g., in the access network, may be desirable in disaster situations with intermittent network connectivity and RFC 5223 offers this capability.

Even though it is technically possible to let seekers and resolvers to enter their queries at any point in the LoST mapping architecture a deployment choice is to configure resolvers with the addresses of the FGs. A query and response for an emergency caller located in Germany with a service provider in Finland could then be shown as depicted in Figure 3. In our example we assume that the VSP deploys a LoST resolver that is contacted by their own customers, the seekers. We furthermore assume in this example that no caching takes place to illustrate the message flow (as shown with dotted lines). In message (1) the seeker contacts its pre-configured resolver with a recursive query providing its current location (somewhere in Germany). The resolver at this point in time does not have any information about the PSAP that has to be contacted for the given location in Germany (for the solicited service). Since the resolver knows the address of the forest guide (only one forest guide is shown in our example) it issues an iterative query to it, as marked with message (2). The FG responds with the entry point for the German LoST tree. The resolver then issues another query towards the provided tree root in message (3). For this example we assume that the root of tree 1 knows the address of the PSAP the seeker has to contact. This final response is then forwarded to seeker via the resolver. The resolver would want to cache the intermediate and final results in order to speed-up later lookups for the same geographical area and the same service. Once the seeker knows the final answer it can proceed with the emergency call setup procedure to contact the PSAP, as shown in message (4) with the double line. As illustrated LoST servers form a distributed mapping database, with each server carrying mapping elements. These mapping elements are the main data structure that is communicated in the LoST protocol, synchronized between FGs, and LoST servers in the tree, and cached by resolvers and seekers. Figure 4 shows the data elements of this important data structure graphically.

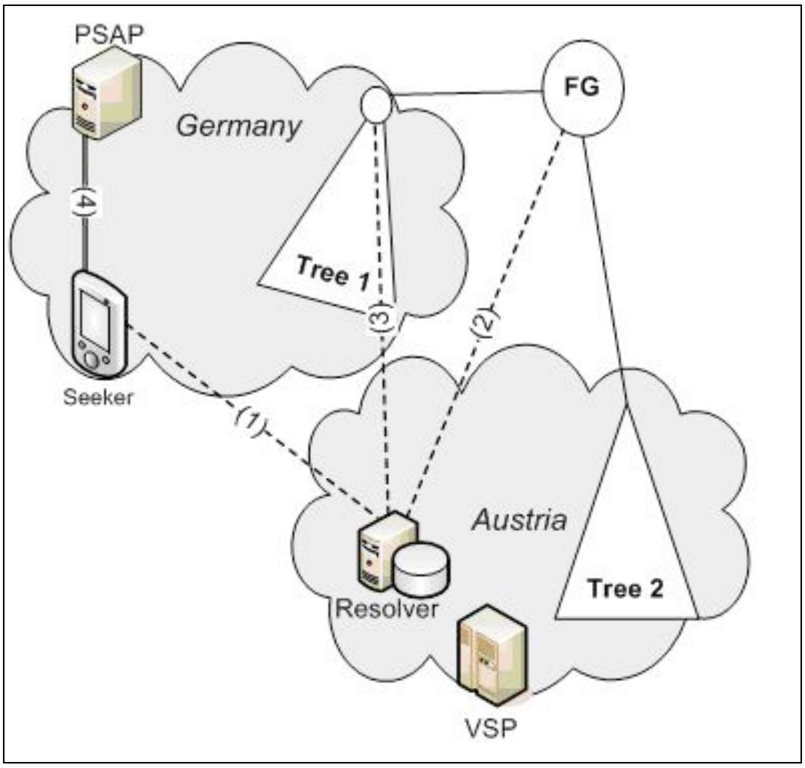


Figure 3: Example Query / Response in the LoST Mapping Architecture.

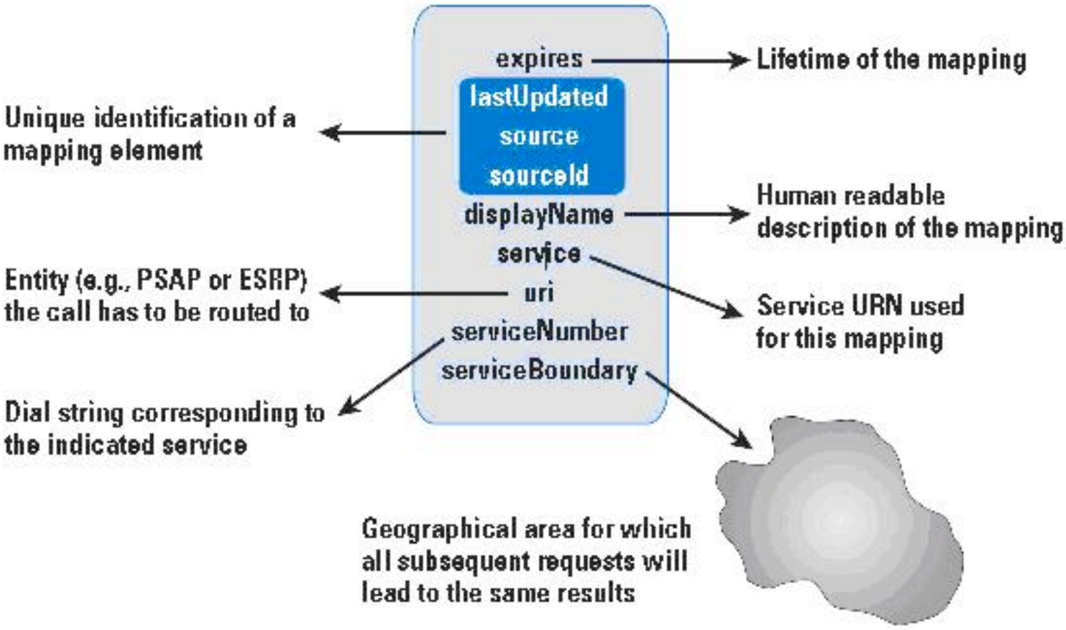

expires
lastUpdated
source
sourceId
displayName
service
uri
serviceNumber
serviceBoundary
Lifetime of the mapping
Unique identification of a mapping element
Human readable description of the mapping
Entity (e.g., PSAP or ESRP) the call has to be routed to
Service URN used for this mapping
Dial string corresponding to the indicated service
Geographical area for which all subsequent requests will lead to the same results

Figure 4: Mapping Element.

5.6 Event Notification

Events are communicated within and between ESInets using the SIP Subscribe/Notify mechanism RFC3265 [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.

NG112 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.

The following events may be implemented in any functional element.

5.6.1 Security Posture

SecurityPosture is an event that represents a downstream entity's current security state. This document uses the European Emergency Services Registry Service (ERS) concept 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: EES-SecurityPosture

Event Package Parameters: None

SUBSCRIBE Bodies: standard RFC4661 + extensions filter specification may be present

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

NOTIFY Bodies: MIME type application/vnd,EES.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 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.

5.6.2 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 with initial defined states of:

- Normal: The element is operating normally, accepting calls and events
- Unmanned: (applies to PSAPs only) The PSAP has indicated that it is not currently answering calls.
- ScheduledMaintenance: The element is undergoing maintenance activities and is not processing calls
- ServiceDisruption: The element has significant problems and is unable to answer calls
- MajorIncidentInProgress: The element is operating normally, but is handling a major incident and may be unable to accept some kinds of calls
- Overloaded: The element is completely overloaded
- GoingDown: The element is being taken out of service
- Down: The element is unavailable
- ComingUp: the element is being put back in service

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: EES-ElementState

Event Package Parameters: None

SUBSCRIBE Bodies: standard RFC4661 + extensions filter specification may be present

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

NOTIFY Bodies: MIME type application/vnd,EES.ElementState+xml

Parameter	**Condition**	**Description**
State	Mandatory	Enumeration of current state from NRS ElementState registry

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).

Notifier Generation of NOTIFY Requests

When the state of the element changes, 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

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.

5.6.3 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 with initial defined states of:

- Normal: The service is operating normally
- 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 reliability
- ServiceDisruption: The service has significant problems and is unable to respond
- Slow: The service is operating normally, but is handling a larger than normal number of requests, responses may be slow.
- GoingDown: The service is being taken out of service
- Down: The service is unavailable
- ComingUp: The service is being put back in service

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: EES-ServiceState

Event Package Parameters: None

SUBSCRIBE Bodies: standard RFC4661 + extensions filter specification may be present

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

NOTIFY Bodies: MIME type application/vnd,EES.ServiceState+xml

Parameter	**Condition**	**Description**
Service	Mandatory	Name of Service
State	Mandatory	Enumeration of current state from NRS ServiceState registry

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).

Notifier Generation of NOTIFY Requests

When the state of the service changes, 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

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.

5.7 Synchronization of Mapping Data

This specification makes use of the LoST Sync specification for replication of mapping information between ECRFs.

5.8 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 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 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 or a Service Database Provider
- A PSAP or ESRP needs to file a DR on a CIDB, or AdditionalLocationData building owner/tenant
- 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 log service
- Any entity may have to file a DR on another entity due to authentication issues (bad certificate, unknown entity, …)
- 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

Next Generation 112 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.

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 and estimates 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 includes:

- 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

5.8.1 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 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
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 response to the Discrepancy Report includes the following;

DiscrepancyReportResponse

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
Comment	Optional	Text comment
errorCode	Optional	Error Code

Error Codes

100	Okay No error
520	Unknown Service/Database ("not ours")
521	Unauthorized Reporter
504	Unspecified Error

5.8.2 Status Update

A reporting agency may request a status update, the update report 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
Comment	Optional	Text Comment

The status report update 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

Comment	Optional	Text Comment
errorCode	Optional	Error Code

Error Codes

100	Okay No error
522	Unknown ReportId
521	Unauthorized Reporter
504	Unspecified Error

5.8.3 Discrepancy Resolution

The reporting agency can query for resolution to any of its outstanding reports. If any responses are available, they will be returned. A query key is passed in the request, and an updated one is returned in the response. The returned query key is used in a subsequent request.

DiscrepancyResolutionRequest is defined as:

Parameter	Condition	Description
QueryKey	Mandatory	Key value returned on previous response
ReportingAgency	Mandatory	Domain name of agency creating the report

DiscrepancyResolutionResponse is defined as:

Parameter	Condition	Description
QueryKey	Mandatory	Key value to be used on next request
ResolutionReport	Conditional	Resolution Report, if available. May be repeated
errorCode	Optional	Error Code

Error Codes

100	Okay No error

524 Bad Query Key

504 Unspecified Error

ResolutionReport is defined as:

Element	Type	Description
ReportId	AN	
ReportingAgency	AgencyId	Domain name of agency creating the report
ReportingAgent	AgentId	UserId of agent creating the report
Service	Conditional	Name of service or instance
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
Timestamp	Timestamp	Date and Time of response
Comment	Optional	Text Comment
Response	Extension	Database/Service-specific response data

The following elements must be included, with the prolog, depending on the service.

5.8.4 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 is invalid, when the client believes it is valid.

LVFDiscrepancyReport is defined as:

Element	Type	Description

Location	PIDF	Location queried
Service	URN	Service URN queried
LocationValidation	LocationValidation (from RFC5222)	Validation Response
Discrepancy	Enumeration	BelievedValid,OtherReport

LVFDiscrepancyResponse is defined as:

Element	Type	Description
ValidationResponse	Enumeration	EntryAdded, NoSuchLocation, OtherResponse

5.8.5 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	Type	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
RetreivePolicyResponse	Mandatory	The Response received from the Policy Retrieve Request as shown in 4.4.1

The PolicyDiscrepancyResponse is defined as:

Element	Type	Description

ValidationResponse	Enumeration	Policy Added, Policy Updated, No Such Policy, Other Response

6 Security

6.1 Introduction

Throughout this document we discuss how IP networks and the SIP-based communication infrastructure creates the foundation on top of which emergency services support is added via a number of building blocks. The building blocks provide the basis for (a) obtaining location information, (b) recognizing an emergency call, (c) evaluating the route towards the PSAP, (d) establishing the SIP session setup and (e) exchanging multi-media data traffic (such as voice, video, text messages, and real-time text).

When considering the security properties of the overall emergency services system two observations can be made.

1. Emergency services support builds on top of the regular communication infrastructure and therefore the security properties of the underlying infrastructure are inherited.
2. Security has to be taken into consideration for each and every protocol since the resulting system is as secure as the weakest link. This also implies that the security analysis done for each protocol has to be taken into account by the respective users of those protocols. Considering point (1) it is easy to observe that there are many protocols involved that need to be examined.

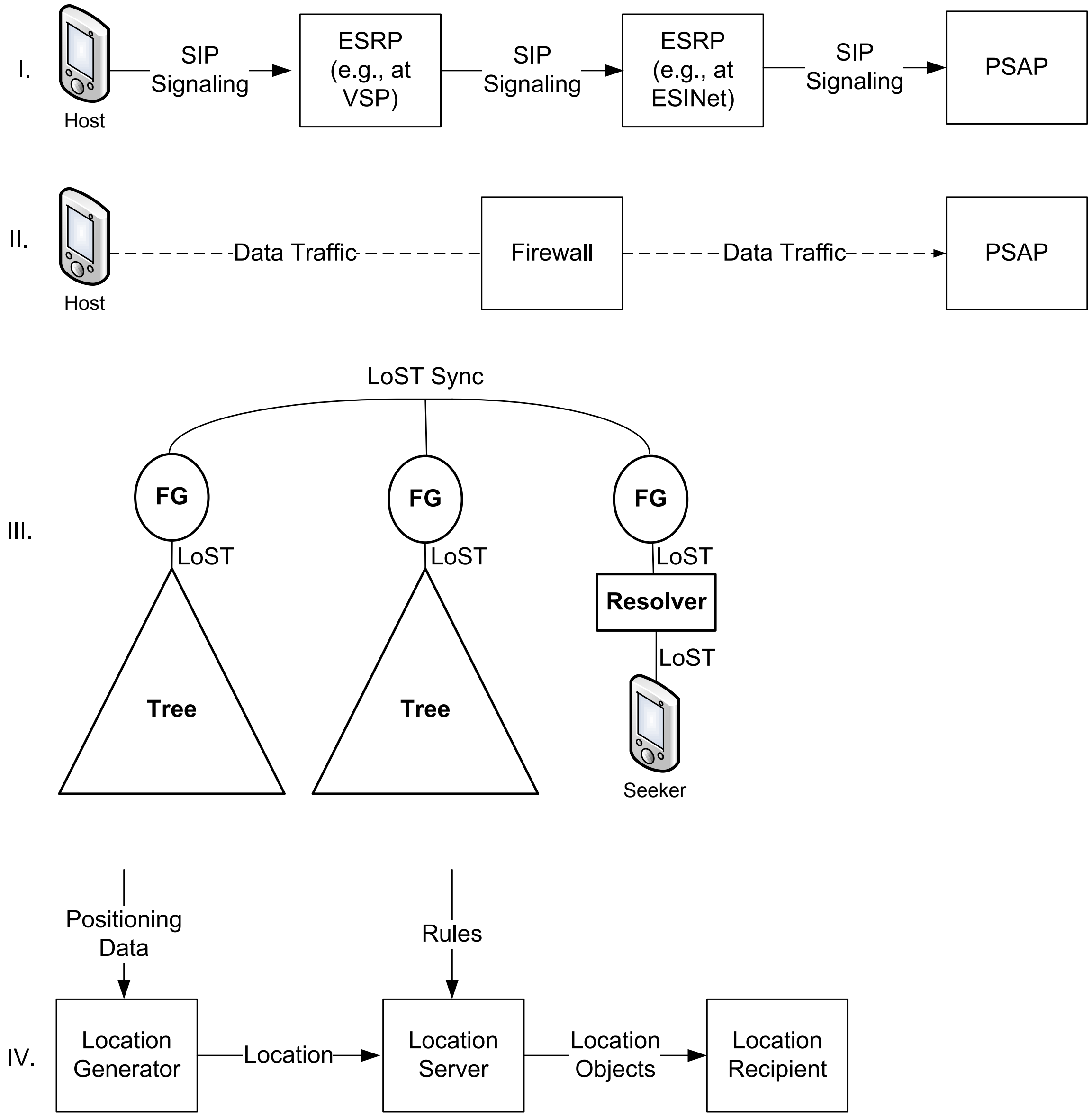
Note: It is not sufficient to write interoperable protocol specifications in such a way that they contain security consideration sections that take the deployment reality into account and at the same time offer an adequate level of protection. But implementations of these protocols also need to be hardened against various implementation bugs, such as buffer overflows, and the deployed system is configured in the appropriate way (e.g., configured with appropriate access control policies to prevent unauthorized access). Building secure communication systems that include emergency services components is complex and presumes education (e.g., via employee training), good software management practices (e.g., secure coding, extensive testing), established and working processes (e.g., incident management, clearly defined responsibilities and accountability), etc. A detailed discussion of these tasks is, however, outside the scope of this document. Hence, we focus our description on the protocol-based mechanisms, which build the basis for any system design. Building communication systems based on global standards, as those described in this document, also ensures that many experts have had an opportunity to review the underlying protocols to identify unexpected side-effects and determine counter-measures.

In this section we will discuss some of the unique security characteristics found in the emergency services environment. First, we start with the description of the communication model and the involved entities of the system, then we investigate the adversary model and security threats. Finally, we conclude with a list of countermeasures.

6.2 Communication Model

When we look at earlier sections, it becomes clear that to evaluate the entire number of protocol interactions of an entire communication system (especially one that also aims to interwork with legacy infrastructure) then it becomes difficult to judge the threats and countermeasures. For this reason we look at the high-level communication models, as shown in the figure below[19].

[19] In this document we use the term 'Location Server' as well as 'Location Information Server' (LIS). RFC 6280 [156] describes the LIS as follows: "Some entities performing the LG role are designed only to provide Targets with their own locations, as opposed to distributing a Target's location to others. The process of providing a Target with its own location is known within Geopriv as Location Configuration. The term 'Location Information Server' (LIS) is often used to describe the entity that performs this function. However, a LIS may also perform other functions, such as providing a Target's location to other entities." In this section we sometimes use the term LIS instead of Location Server.



There are four main communication interactions to consider:

- SIP Signaling Communication: The SIP signaling exchange is at the heart of the emergency services communication. SIP is an application-layer control (signaling) protocol for creating, modifying, and terminating sessions with one or more participants. The emergency services functionality is added to SIP with specifications that allow emergency services functionality to be expressed (using the Service URN specification in RFC 5031 [58]) and the ability to carry location objects in SIP (see [204]). The additional functionality needed for emergency call signaling that had to be added to the already feature-rich SIP protocol was fairly small and most effort was spent on the responsibilities of the different stakeholders in the overall architecture. After the emergency services communication terminates it is possible for the PSAP to initiate a callback to the originatior of the emergency call, for example when important details about the emergency situation have not been clarified or the caller prematurely terminated the conversation. The call setup procedure then starts with the PSAP and the SIP session setup messages traveling towards the end device that initiated the original call.

- Exchange of Multi-Media Data: The main purpose of the communication setup is to exchange data. For emergency calls this typically takes the form of voice packets but will in the future with the capabilities of IP also be video, instant messages, realtime text, and pictures. SIP is able to negotiate the functionality supported by both sides, and to enable the exchange of these various media streams. The media used will largely depend on the capabilities of the devices, the installed software applications, and the preferences of the emergency caller. For persons with disabilities, real-time text and video communication is likely to make a big difference but might require a third party relay service to be invoked, for example, for sign language interpretation. Note that the SIP signaling may also indicate properties of the media, such as the human language preferences (e.g., audio with French, or video with American Sign Language).
- Mapping Database: When emergency call setup is initiated then the call routing processes need to make a decision about which next hop to route the setup messages to. A major influencing factor in call routing is location information since in many regions the appropriate PSAP is determined by the location of the caller. In some cases, other factors, such as load situation at a PSAP or the ability to accept certain media types will influence the decision. For location based routing, the distributed mapping database that uses the protocol LoST is used, as illustrated in [60,61]. The design is similar to that of the DNS and allows various hosts and ESRPs to ask for the appropriate PSAP based on a given location input.
- Location Infrastructure: The location retrieval interaction starts with some entity issuing a request for a location object. The requesting party is the Location Recipient, which may be the end host, a VSP proxy, an ESRP, or the PSAP. All these entities have a legitimate interest in receiving location information for subsequent consumption for determining the appropriate emergency dial strings, for emergency call routing, or for dispatch of first responders. When a location server, which is commonly assumed to be operated by an ISP, receives a location request it may not always have the most current information cached; it may therefore need to start a location determination process whereby location generators collect positioning data. The location server may also provide location information not only as a one-

shot transaction but might be ask to repeatedly provide updates, for example as location determination techniques compute better location over time or when the location of the target device changes. For security and privacy purposes location may not be handed out to everyone without a prior authorization check, which will be determined based on a rule set available to the location server. This architecture allows several location configuration protocols to be used and RFC 6280 [156] provides a high level description of the different variants and introduces terminology.

6.3 Adversary Models and Security Threats

In a discussion about security threats it is important to keep the anticipated capabilities of an adversary in mind. We distinguish between three types of adversaries:

- **External Adversary Model**: This type of adversary is the most commonly considered adversary in communication networks. The adversary is external to the analyzed system and interferes from the outside. In such a threat model it is assumed that none of the emergency service infrastructure elements had been compromised. As an example of the type of analysis to be performed consider the case where a person makes an emergency call. An adversary could be located along the communication path between the end host and the location server, or between the end host and the PSAP. Without proper communication security employed this adversary could be capable in eavesdropping on the communication, modifying information (such as origination, call-back, location, media) or preventing the emergency caller from successfully calling for help.
- **Malicious Infrastructure Adversary Model**: With this type of adversary model we assume that some entities in the emergency services infrastructure may either be misconfigured and thereby disrupt the normal emergency system operation or that some components are compromised and under the control of an attacker. For example, elements used in the process to route emergency calls, such as the LIS, the Location-to-Service Translation (LoST) infrastructure [60,61], used for mapping locations to a PSAP address, or call routing elements, may be manipulated to respond with false information.
- **Malicious End Host Adversary Model**: With this adversary model we assume that the end system is compromised. Although this type of adversary model is a sub-category of the malicious infrastructure adversary model it deserves special attention since end systems, such as tablets and desktop PCs, are often more vulnerable (e.g., due to their software update policy or lack of skilled administration). Furthermore, a human interacting with the emergency services authorities may have intentions that are not aligned with the call takers or the first responders. We will discuss these problems in context of hoax calls.

While we do not explicitly call out the different adversary models when we describe individual security threats but in our description we explain the assumptions that need to be met for a successful attack.

6.4 Security Threats

As a starting point we have to think about the motivations of an attacker and to speculate about their available resources to launch such an attack. While some attacks are likely going to be "carried over" from the existing telephony system, others will be new due to the additional capabilities offered by IP-based emergency services systems.

Attackers may direct their efforts either against a portion of the emergency response system or against an individual. Attacks against the emergency response system have three possible objectives:

- to deny system services to all users in a given area. The motivation may range from thoughtless vandalism, to wide-scale criminality, to terrorism.
- to convey prank calls to PSAP call takers and first responders. A fairly small number of prank calls may consume an enormous amount of resources from the emergency services infrastructure. While there are many variations of these prank and hoax calls, a severe version is called "Swatting" and is where an adversary simulates the commission of a punishable offense (such as a hijacking situation) and at the same time fools the emergency services system in using wrong location information for dispatching police units. The name derives from the term “SWAT”, an acronym for *Special Weapons and Tactics*, used to denote specialized police units deployed for high-risk situations where snipers, high-caliber weapons, and other less-common responses may be appropriate. The goal of a swatting attack is generally to cause a swat team to be dispatched to the location of an innocent individual or group, often with intent for deadly interactions.

One can certainly imagine other, more exotic types of attacks. For example, an attacker could

- divert emergency calls to non-emergency sites. This is a form of a denial-of-service attack that will quite likely be very confusing for the emergency caller since he or she expects to talk to a PSAP operator but instead gets connected to someone else.
- to gain fraudulent use of services, by using an emergency identifier to bypass normal authentication, authorization, and accounting procedures. The goal of the adversary with such an attack is to gain a financial advantage.
- to get elevated priority treatment in the hope to gain faster service by blocking others’ competing calls for help.

Attacks against an individual may have the following motivation:

- to prevent an individual from receiving aid.
- to gain information about an emergency that can be applied either against an individual involved in that emergency or to the profit of the attacker.
- to deliver unwanted messages to a non-emergency caller using technologies developed for emergency services purposes, for example the PSAP callback mechanism, to bypass authorization policies.
- to use technology designed for emergency services purpose for turning a user’s phone into a recording device.
- to use sensitive personal data (e.g., health records) for non-emergency services purposes, or to retrain personal data beyond an acceptable retention period.
- to disclose location information without prior consent to third parties by bypassing the access control mechanism of a location server.

In the subsections below we describe a few attacks in more detail. The list is not exhaustive but illustrates concerns frequently raised.

6.4.1 Denial of Service Attacks

Emergency services have at least three finite resources subject to denial of service attacks: the network and server infrastructure, call takers, and first responders, such as fire fighters and police officers. The task of protecting network and server infrastructure shares similarities with high-value e-commerce sites and lessons can be learned from these environments particularly regarding capacity planning, load balancing, DDoS prevention techniques, and abuse reporting. Call takers are a far more limited resource; even large cities might only have PSAPs with only a handful of PSAP call takers on duty. Even if the call takers attempt to question the caller to weed out prank calls, they would be quickly overwhelmed by even a small-scale attack. Finally, first responder resources are limited as well and since every assignment takes an extended period of time their resources are quickly dried up, not only during mass-casualty events.

6.4.2 Attacks Involving the Emergency Identifier

The overall process of establishing an emergency call begins with the person in need for help dialing the emergency dial string. The exact sequence of digits depends on the infrastructure the device is connected to. Although 1-1-2 became the emergency services number for Europe, and 911 for the US, many countries still provide emergency numbers in addition to the 112/911. Furthermore, many large enterprises, university, and hotels prefix the emergency numbers with additional digits, such as 0-112, or 9-911. It is therefore important for devices that can be used in different environments, or a SIP proxy used by such devices, to automatically detect which dial string triggers an emergency call. Pre-programming the list of numbers in use world-wide is not possible due to the overlap of emergency and non-emergency numbers.

With dial strings there are two challenges to solve:

1. A device needs to have the capability to learn their emergency services numbers available for a specific attachment point. LoST provides a mechanism for obtaining the emergency dial string for a given location.
2. For unambiguous processing of protocol messages it is useful to replace the actual dial string with a symbolic name. This is accomplished with Service URNs, see RFC 5031 [58]. Calls marked with this emergency identifier are then treated as emergency calls by the call routing entities by giving them special treatment. An example of a service URN is "urn:service:sos.police". In combination with LoST's ability to learn the dial string for a given location this allows a device to dynamically translate emergency dial strings to Service URNs for usage in emergency calls.

Users, however, do not "dial" an emergency URN itself. Instead, the entered emergency dial strings are translated to corresponding Service URNs, carried in the Request-URI of the INVITE request. This translation should ideally be done at the end point because the need to detect an emergency call at the end host is required, for example, to perform an emergency registration with a cellular network, convey location in the signaling, or to disable specific call features (e.g., noise cancellation) or enable emergency-specific ones (e.g., not drawing extra attention during text message exchanges). Once a call is marked with an "sos" Service URN, call routing entities give it preferential treatment.

The main possibility of attack involves use of the emergency identifier to bypass the normal procedures in order to achieve fraudulent use of services. An attack of this sort is possible only if the following conditions are true:

- The attacker is faking an emergency call.
- The call enters the domain of a service provider, which accepts it without applying normal procedures for authentication and authorization because the signaling carries the emergency identifier.
- The service provider routes the call according to the called address (e.g., SIP Request-URI), without verifying that this is the address of a PSAP (noting that a URI by itself does not indicate the nature of the entity it is pointing to).

If these conditions are satisfied, the attacker can bypass normal service provider authorization procedures for arbitrary destinations, simply by reprogramming the emergency caller's device to add the emergency identifier to non-emergency call signaling. When using the Resource Priority Headers for emergency communications [47,157] then a call routing device may also be tricked into using this information as the sole basis for bypassing authentication, or authorization procedures. This would also allow an adversary to use this indication to gain preferential treatment of marked traffic that is of greater preference within a network than other traffic.

6.4.3 Attacks Against the Mapping System

This section considers attacks intended to reduce the effectiveness of the emergency response system for all callers in a given area. If the mapping operation is disabled, then the correct functioning of the emergency call routing infrastructure cannot be guaranteed. As a consequence, the probability that emergency calls will be routed to the wrong PSAP increases. Routing calls to the wrong PSAP may have two consequences: emergency response to the affected calls is delayed, and PSAP call taker resources outside the immediate area of the emergency are consumed due to the extra effort required to redirect the calls.

Alternatively, attacks that cause the client to receive a URI that does not lead to a PSAP have the immediate effect of causing emergency calls to fail.

Three basic attacks on the mapping process can be identified: denial of service, impersonation of the mapping server, or corruption of the mapping database. Denial of service can be achieved in several ways:

- by a flooding attack on the mapping server;
- by taking control of the mapping server and either preventing it from responding or causing it to send incorrect responses;
- by taking control of any intermediary node (for example, a router) through which the mapping queries and responses pass, and then using that control to block them. An adversary may also attempt to modify the mapping protocol signaling messages. Additionally, the adversary may be able to replay past communication exchanges to fool an emergency caller by returning incorrect results.

In an impersonation attack, the attacker induces the mapping client to direct its queries to a host under the attacker's control rather than the real mapping server, or the attacker suppresses the response from the real mapping server and sends a spoofed response. The former type of impersonation attack itself is an issue of mapping server discovery rather than the mapping protocol directly. However, the mapping protocol may allow impersonation to be detected, thereby preventing acceptance of responses from an impersonating entity and possibly triggering a more secure discovery procedure.

Injecting fake mapping entities into the distributed mapping database may lead to an inconsistent state of the distributed database. If an adversary manages to inject false mappings then this could lead to denial of service attacks. If the mapping data contains a URL that does not exist then emergency services for the indicated area are not reachable. If all mapping data contains URLs that point to a single PSAP (rather than a large number) then this PSAP is likely to experience overload conditions. If the mapping data contains a URL that points to a server controlled by the adversary itself then it might impersonate PSAPs.

6.4.4 Attacks against the Location Information Server

A LIS provides information end hosts and other entities in the system, which is then used for routing of emergency calls and for dispatching first responders. The LIS itself often has to obtain information from other sources to compute the location of an end system in an iterative fashion.

An adversary who wants to provide false location to a PSAP has a number of choices. Tampering with location information is one possible choice and interfering with the location determination procedure executed by a LIS is another possible approach. The process of determining location information heavily depends on the specific network deployment but at an abstract level the process is fairly simple: A Location Recipient, like the end host or an ESRP, transmits a request for location information to a LIS. Some information about the device to be located has to be provided in that request to allow the LIS to do its job. Unfortunately, there is no unique device identifier available that ideally fulfills that purpose. The Location Recipients have a few identifiers to choose from; the IP address is commonly used. In other cases more identifiers are available, for example those listed in [104] include a MAC address, a Network Access Identifier, and the DHCP Unique Identifier. When a LIS receives such a request for location information it will have to associate the obtained identifier with information available in its databases. The data may have been manually provisioned but will typically be collected automatically from normal network operation, such as network management, network attachment procedures and mobility protocols. For example, a LIS located in a DSL network receives a request asking for location related to a specific IP address. The IP address may be allocated from a pool of addresses maintained by the Authentication, Authorization and Accounting (AAA) server and therefore the AAA server has to be queried. The AAA may know the current attachment point of the end host or may use available information about the DSL Access Module (DSLAM) and Access Node (AN) and the related identifiers (e.g., to determine the position of the end host Ethernet VLAN tags, Layer 2 tunnel identifiers, virtual port ID (VPI) and virtual circuit ID (VCI)). Further examples of such measurement identifiers are provided in [158].

Consequently, there are various methods by which an adversary can interfere with the process of resolving a chain of identifiers to finally obtain location information. If the adversary succeeds in feeding incorrect information in the lookup step, it may be able to fool a LIS into handing out wrong location information. Examples of interfering with identifier mapping include the sending of a false MAC address or an IP address to obtain different location information. It should also be noted that wiremap maintenance is prone to errors thereby resulting in wrong information being handed out even in the absence of malice.

An adversary may also be able to cause an emergency call to carry a location URI pointing to a compromised LIS (e.g., a LIS under the adversary’s control).

6.4.5 Swatting

Prank calls have been a problem for emergency services, dating back to the time of street corner call boxes. Individual prank calls waste scarce emergency service resources and possibly endanger bystanders or emergency service personnel as they rush to the reported scene of a fire or accident. Risks to human life are not a typical security threat withing communication protocols. Emergency services are, however, different in this regard.

Recent 'swatting' incidents with life threatening consequences have captured media attention [160]. Some of these incidents have involved spoofing of the originating phone number when calling an emergency number. This leads to a location lookup for the wrong location since the input to the location determination process is the phone number in legacy fixed deployments. This could result in a SWAT team being dispatched to the location of a completely innocent citizen, if the swatter is able to convince the call taker that a serious crime is under way. The FBI has warned about the increasing prevalence of swatting incidents [159].

Legacy emergency services rely on the ability to identify callers, as well as on the difficulty of location spoofing for normal users to limit prank calls. The ability to ascertain identity is important, since the threat of severe punishments reduces prank calls. Mechanically placing a large number of emergency calls that appear to come from different locations is difficult. Calls from pay phones are subject to greater scrutiny by the call taker.

In the current system, it would be very difficult for an attacker from country 'Foo' to attack the emergency services infrastructure located in country 'Bar'.

In countries that do not allow SIM-less emergency calls, i.e., emergency calls that are made without any authentication, the identity of most callers can be ascertained, so that the threat of severe punishments reduces prank calls. As a comparison, in countries where SIM-less emergency calls are allowed phrank calls may be as high as 50%.

There is concern that VoIP systems further simplify these types of phrank calls when identities and location information can easily be crafted. It may even be possible to have attackers located in one country attack the emergency services infrastructure located in a different country or to mechanically (e.g., with the help of bot nets) initiate a large number of emergency calls that appear to come from different locations.

6.4.6 Attacks to Prevent a Specific Individual from Receiving Aid

If an attacker wishes to deny emergency service to a specific individual, the mass attacks described earlier will obviously work provided that the target individual is within the affected population. Except for the flooding attack on the mapping infrastructure, the attacker may also want to focus on a specific individual. To guarantee effectivenes an adversary may attack the end device directly rather than the emergency services infrastructure.

The choices available to the attacker are

- to take control of any intermediary node (for example, a WLAN router at the user's home). Absent further security mechanisms this allows the adversary to modify requests and responses or to even block the entire communication.
- to interfere with the communication of the end device and other emergency service entities, for example, over the WLAN home network
- to infect the user's device with malware and consequently to have full control over the device.

In general, these type of attacks are difficult to prevent by an emergency services system itself and require improvments for Internet security in general.

6.4.7 Attacks to Gain Information about an Emergency

This section discusses attacks used to gain information about an emergency. The attacker may be seeking the location of the caller (e.g., to effect a criminal attack) or to use information to link an individual (the caller or someone else involved in the emergency) with embarrassing information related to the emergency (e.g., "Who did the police take away just now?"). Finally, the attacker could take profit from the emergency, perhaps by offering his or her services (e.g., a news reporter, or a lawyer aggressively seeking new business).

The primary information that interceptions of mapping requests and responses will reveal are a location, a URI identifying a PSAP, the emergency service identifier, and the addresses of the mapping client and server. The location information can be directly useful to an attacker if the attacker has high assurance that the observed query is related to an emergency involving the target. The type of emergency (fire, police, or ambulance) might also be revealed by the emergency service identifier in the mapping query. The other pieces of information may provide the basis for further attacks on emergency call routing. The attacker may gain information that allows for interference with the call after it has been set up or for interception of the media stream between the caller and the PSAP.

Finally, the attacker may gain access to the conversation between the emergency caller and the call taker rather than just the meta-data about the incident.

6.4.8 Interfering with the LIS and LoST Server Discovery Procedure

Many entities in the emergency services architecture are configurable to offer some amount of flexibility. Dynamic discovery procedures have been developed to avoid manual configuration. The LIS, and the LoST server discovery are examples.

The primary attack against the discovery step is impersonation. When there is no natural a-priori relationship between the two devices then the attack surface is increased. End devices, for example, are not supposed to be pre-configured manually with a LIS located in their ISPs network. Particularly, for mobile devices such a LIS would frequently change as they change their point of attachment. In case of LoST, however, an end device may be statically provisioned to use a single

LoST server all the time. Similiarly to the DNS it is, however, possible to discover and use a local LoST sever, which would provide improved resilience.

An attacker could attempt to compromise LIS and LoST discovery at any of three stages:

1. providing a falsified domain name to be used as input to U-NAPTR
2. altering the DNS records used in U-NAPTR resolution
3. impersonation of the LIS

U-NAPTR is entirely dependent on its inputs. In falsifying a domain name, an attacker avoids any later protections, bypassing them entirely. To ensure that the access network domain name DHCP option can be relied upon, preventing DHCP messages from being modified or spoofed by attackers is necessary.

Once a client has been tricked into talking with the wrong LIS or LoST server subsequent steps for emergency service protocol execution are at risk to fail or to be manipulated in favor of the adversary.

6.4.9 Call Identity Spoofing

If an adversary can place emergency calls without disclosing its identity, then determining the source of prank calls nay be more difficult. There are at least two different forms of authentication and authorization in this context:

- Authentication at the link layer or at the network layer (e.g., using the Extensible Authentication Protocol (EAP))
- Authentication at the application layer, for example at the VoIP application.

Note that this split is possible when there is separation between the ISP and the VSP. Since two different stakeholders manage the identity space, the identities used during authentication are different as well. While not all architectures assume such a separation of roles, they are nevertheless common on the Internet today.

Whenever misuse occurs and a PSAP call taker or the emergency services authorities would like to pinpoint someone, the first observation is that they do not authenticate any emergency caller themselves. However, two other stakeholders along the communication chain may do so: the VSP and the ISP. Even with proper authentication at the VSP or the ISP, there is additionally the question of how strong the prior identity proofing step was, i.e., what a customer has to do in order to create an account with an ISP or VSP to use their communication servers. The quality of identity proofing must not be ignored since it provides the link of a digital identity to the identity of a person in the real world.

In case of misuse, the emergency services authorities first have to interact with the VSP and/or the ISP to identify a particular individual. In certain cases there is no authentication procedure executed and hence this re-identification can be challenging. This might, for example, be the case with an open IEEE 802.11 WLAN hotspot. While the owner of the WLAN hotspot can be determined this may be insufficient for determining the adversary utilizing this WLAN network.

Given the importance of authentication for ensuring accountability in case of misuse, mistakes made in the legacy telephony network can be fixed. In particular, the ability to make emergency calls without any form of authentication or by utilizing caller-id spoofing can be reduced by various technical means, education about the negative side-effects, and by regulatory frameworks. Mandating authentication for emergency calls, and even the introduction of special credentials, for example an emergency certificate, is imaginable. Needless to say that a dedicated security mechanisms increase costs, introduces an administrative overhead and are only, from a security point of view, useful when widely used.

6.5 Countermeasures

In the previous section we illustrated a few attacks on the emergency services system and with the writeup in this section we are aiming to highlight a number of techniques to mitigate these threats.

6.5.1 Discovery

Physical or link layer security are commonplace methods for securing the initial communication link between an end device and the network infrastructure to reduce the possibility of attack particularly at the early phases of the communication establishment. These link layer security mechanisms are particularly useful in those cases where location information is directly exchanged via DHCP. While DHCP offers its own security mechanism, see RFC 3118, it is impractical for deployments. However, for the interaction with HELD or LoST additional security capabilities are available at higher protocol layers since these protocols run over HTTP and TLS.

LoST and HELD intentionally share a very similar discovery mechanism that can be used by end devices as well as by intermediate entities, like emergency services routing proxies.

As a summary, an end device performs the following steps (in case of a dynamic discovery of a LIS and a LoST server in the access network):

1. Acquire the access network domain name. DHCP can provide the end host with a domain name.
2. This domain name is then used as input to the DNS-based resolution mechanism. For LoST this resolution mechanism is described in RFC 5222 [61] and for HELD it is defined in RFC 5986 [160]. In both cases the URI-enabled NAPTR specification is used.

An ESRP may also need to discover the network domain name for a LIS (as it is the case in transition scenarios where no Location by Reference is available) but it cannot rely on DHCP for that purpose. Transition architectures may use alternative approaches for discovering the access network domain of a LIS. For a LoST server discovery the ESRP will be pre-configured with a domain name, which simplifies discovery since every LoST is able to receive a correct answer from the distributed mapping database.

To avoid an attacker modifying the query or its result of any interaction with a LIS or a LoST server, Transport Layer Security (TLS) is strongly recommended. For LoST there is the additional concern that operating without TLS allows cache poisoning since LoST has a built-in caching mechanism.

The entity interacting with a LoST server or a LIS has to check the TLS server's identity, as described in Section 3.1 of RFC 2818 [161]. Omitting the server identity check should be used only when getting any answer, even from a potentially malicious LIS or LoST server, is preferred over closing the connection (and thus not getting any answer at all) since it allows an attacker to masquerade as a LIS or LoST server.

The domain name that is used to authenticate the LIS or LoST server is the domain name in the URI, i.e., the result of the U-NAPTR resolution, and it is compared against the server's certificate. To phrase it differently, when the access network domain name is 'example.com' and the U-NAPTR lookup leads to a https://lostserver.example.com URL then the certificate provided by that server has to contain the lostserver.example.com name.

Therefore, if an attacker modifies any of the DNS records used in the resolution process, this URI could be replaced by an invalid URI.

DNS Security (DNSSEC) can be used to protect against these threats. While DNSSEC is not yet completely deployed, users should be aware of the risk, particularly when they are requesting NAPTR records in environments where the local recursive name server, or the network between the client and the local recursive name server, is not considered trustworthy. Security considerations specific to U-NAPTR are described in more detail in [164].

LoST deployments that are unable to use DNSSEC and unwilling to trust DNS resolution without DNSSEC cannot use the NATPR-based discovery of LoST servers as is. When suitable configuration mechanisms are available, one possibility is to configure the LoST server URIs (instead of the domain name to be used for NAPTR resolution) directly. Note that this procedure is different to what the security considerations in RFC 3958 [163] recommend. RFC 3958 suggests to compare the input of NAPTR resolution to the certificate, not the output (host name in the URI). This approach was not chosen because in emergency service use cases, it is likely that deployments will see a large number of inputs to the U-NAPTR algorithm resolving to a single server, typically run by a local emergency services authority. Checking the input to the NAPTR resolution against the certificates provided by the LoST server would be impractical, as the list of organizations using it would be large, subject to rapid change, and unknown to the LoST server operator. The use of server identity does leave open the possibility of DNS- based attacks, as the NAPTR records may be altered by an attacker. The attacks include, for example, interception of DNS packets between the client and the recursive name server, DNS cache poisoning, and intentional modifications by the recursive name server; see RFC 3833 [162] for more comprehensive discussion.

Using the domain name in the URI is more compatible with existing HTTP client software, which authenticate servers based on the domain name in the URI. A LIS or LoST server that is identified by an "http:" URI cannot be authenticated. Use of unsecured HTTP also does not meet requirements in HELD for confidentiality and integrity. If an "http:" URI is the product of discovery, this leaves devices vulnerable to several attacks. Lower layer protections, such as layer 2 traffic separation might be used to provide some security guarantees against adversaries on the wireless-interface, but should not be seen as a replacement for application layer security.

Generally, LoST servers will not need to authenticate or authorize clients presenting mapping queries. If they do, an authentication of the underlying transport mechanism, such as HTTP basic and digest authentication, may be used. Basic authentication should only be used in combination with TLS. The usage of TLS with mutual certificate-based authentication is another option for server-to-server communication.

6.5.2 Secure Session Setup and Caller Identity

The Session Initiation Protocol (SIP) and the Session Description Protocol (SDP) are used to set up multimedia sessions or calls. SIP messages travel from the emergency callers device via the intermediate SIP infrastructure towards the call takers device at the PSAP.

The SIP protocol suite offers solutions for securing SIP signaling as well as conveying caller identity information to the called party.

The mechanisms can be clustered into three categories:

1. the process of verifying the user's identity. The VSP's infrastructure elements authenticate the user. This can, for example, happen via the basic SIP authentication mechanisms (such as digest authentication).
2. the process of asserting the previously verified identity to a third party. The authenticated identity is not only important for the VSP but also for end-to-end communication to the remote party. The VSP can assert this identity towards other parties using mechanisms, such as SIP Identity, described in RFC 4474 [166], or P-Asserted-Identity, specified in RFC 3325 [165].
3. SIP signaling security. This ensures that an adversary cannot inject fake signaling messages, eavesdrop on the communication, replay messages, etc. Transport Layer Security (TLS) is used for providing authentication, integrity, and confidentiality protection between neighboring SIP nodes. Since SIP signaling supports multiple transport protocols, not just TCP, Datagram TLS was introduced to allow TLS functionality to datagram transport protocols.

There are two main technologies for communicating identity information in SIP are:

- **P-Asserted-Identity (RFC 3325):** After authenticating the user, the VSP's SIP proxy adds the P-Asserted-Identity (PAI) header to the SIP message. This header carries the authenticated identity (SIP URI) of the user. The P-

Asserted-Identity header is protected only in a hop-by-hop fashion between the SIP proxies along the path. The mechanism can only be used within a trust domain in which the SIP proxies and UAs communicate securely and the proxies are mutually trusted. The design of PAI is therefore based on a chain of trust rather than on a cryptographic end-to-end security solution.

- **SIP Identity (RFC 4474):** SIP Identity extends the PAI concept with a cryptographic identity assurance. SIP messages are sent to an Authentication Service, which is responsible for verifying that the user agent software knows a shared secret, for example using the HTTP Digest authentication protocol. Based on successful user authentication, identity information is written into the From header of the SIP request. This part is identical to the PAI scheme. Then, the Authentication Service adds a digital signature to a new SIP Identity header before forwarding it to the final recipient. Within the forwarded SIP request the Authentication Service also provides a reference (using an HTTP URI in the Identity-Info header) to its own domain certificate. The recipient of the SIP message, for example the call taker's SIP user agent software, performs the following actions to verify the authenticated identity: First, it fetches and validates the certificate of the Authentication Service. Then, it verifies the signature of the SIP message and the identity of the user. Finally, it checks the value of signed Date header to protect against replay attacks.

6.5.3 Media Exchange

The main goal of the communication establishment explained in the previous section is in the exchange of multi-media data between the two (or more) SIP end points. The offered security services do not only need to protect the communication setup but also need to ensure protection of the media exchange. SDP is responsible for negotiating the media and it is a versatile protocol. SDP does not only allow the setup of Real-Time Transport Protocol (RTP), which is mainly used to transmit real-time media on top of UDP and TCP, but is also able to set up TCP and additionally TCP/TLS connections for usage with media sessions.

The Secure RTP (SRTP) [169] is the established standard for securing RTP. In order to allow SRTP to offer its service, cryptographic keys need to be established between the involved communication parties, via a key exchange protocol. Various key exchange protocols have been proposed and analysed [168] and among all the options DTLS-SRTP, described in RFC 5763 [172, 170], was chosen as the preferred IETF mechanism. However, the precursor to DTLS-SRTP, the Security Description (SDES) protocol [167], is widely used today despite its inferior security characteristics.

In order to protect against a number of attacks it is therefore necessary for the SIP communication end points to implement and use a key exchange protocol (and DTLSSRTP and for today's deployment environments also SDES) and SRTP itself.

6.5.4 Mapping Database Security

Throughout this document we make use of a distributed mapping database that uses the LoST protocol and LoST-Sync for distributing mappings between server nodes.

With the protocol exchange of mapping information a minimum requirement is to authenticate neighboring server nodes using available HTTP security mechanisms, such as HTTP Digest [171], HTTP Basic [171] over TLS, or plain TLS with client and server certificates [173].

A minimum amount of manual configuration for the setup of the LoST server relationships is required and hence the choice of the security mechanisms used between the two entities is a deployment specific decision. Nevertheless, the usage of certificates is an attractive option since it allows a Public Key Infrastructure (PKI) with a separate trust anchor to be used. Whenever a new server infrastructure element is introduced a new certificate is obtained and signed by the corresponding CA. This certificate is then ready for usage by the other infrastructure elements without additional administrative configuration burden. In any case, it must be ensured that the two communicating end points authenticate each other and utilize the established secure communication channel (i.e., an integrity protected exchange of data with the help of the TLS Record Layer) to avoid the possibility of injecting bogus mappings.

An entity acting maliciously would, however, intentionally modify mappings or inject bogus mappings. To avoid the possibility of one entity claiming a service boundary belonging to some else, any node introducing a new service boundary must digitally sign the mapping and thereby protecting the data with an XML digital signature. This ensures that a new mapping is associated to a particular owner with non-repudiation properties. Absent any automatic procedures a system administrator must approve the received mapping prior to include it in the database. Determining who can speak for a particular region is inherently difficult unless there is a small set of authorizing entities that all other participants can trust. Receiving systems should be particularly suspicious if an existing coverage region is replaced with a new one containing different contact points. With this end-to-end security mechanism it is nevertheless guaranteed that mappings are modified by servers forwarding them as part of the synchronization procedure.

7 Gateways

While NG1-1-2 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 NG architecture. Since any PSAP will need to be able to receive emergency calls that originate on those legacy networks, and legacy PSAPs will need to process voice emergency call originations that traverse ESInets, it is clear that gateways will be a requirement. The Legacy Network Gateway (LNG) is an 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.

An EENA survey about emergency caller location provisioning revealed heterogeneous PSAP interfaces in existing EU implementations (http://www.EENA.org/view/en/Committees/112operations/index/esaccess.html). Although the majority of EU PSAPs use BRI, PRI or in some cases, SS7 network interfaces, the signaling schemes, and methods of location conveyance utilized (push, pull various different quality of service requirements) differ significantly. Consequently, the NG112 architecture positions the LPG outside of the native architecture to encapsulate heterogeneities.

This results in different NG1-1-2 deployment models to ensure investment protection of existing PSAP legacy CPE, while PSAP interconnectivity via a common NG1-1-2 PSAP interface is accomplished. Besides, the LPG component is designed such that more than one PSAP can be supported, to utilize economies of scale for these bridging technologies and foster migration strategies.

The placement of the gateways in the NG1-1-2 solution architecture and the functional components that make up the Legacy Network Gateway and the Legacy PSAP Gateway are illustrated in Figure 5.

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.

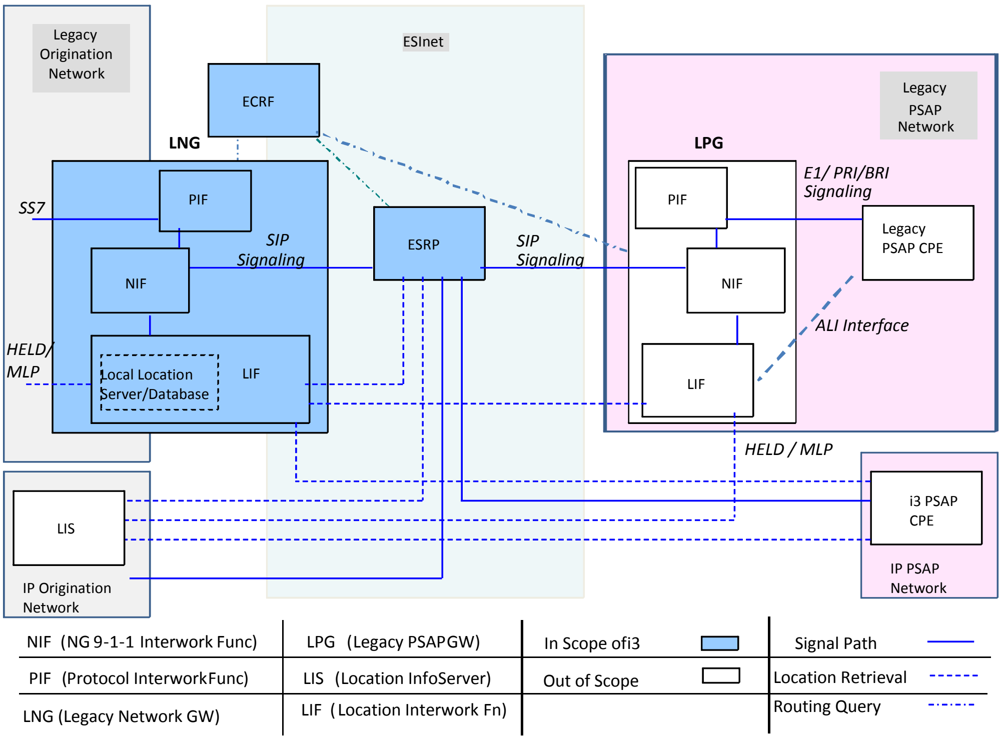


Figure 5: Gateways – Functional Architecture.

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 NG architecture. Logically, the Legacy Network Gateway logically resides between the originating network and the ESInet and allows 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 Signaling System Number 7 (SS7) signaling to the IP-based signaling supported by the ESInet. Thus, the Legacy Network Gateway supports a physical SS7 interface on the side of the originating network, and an IP interface which produces SIP signaling towards the ESInet, and must provide protocol interworking functionality between the SS7 signaling that it receives from the legacy originating network and 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 MSC (e.g., Calling Party Number - CLI) to be used as input data for 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. These functional components are described below:

1. (SS7-to-SIP) Protocol Interworking Function. This functional component performs a standard interworking function that converts the incoming SS7 protocol from the legacy network to the SIP protocol expected by the ESInet and also converts the incoming TDM voice to the RTP data required by the ESInet. It is assumed that the PIF functional component does not require specialized hardware, and can therefore be implemented using commercially available hardware.)
2. NG1-1-2 specific Interwork Function (NIF). This functional component provides NG1-1-2-specific processing of the incoming call signaling, (e.g., calling party number/CLI) 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.
3. Location Interwork Function (LIF). This functional component is responsible for taking the appropriate key(s) from the incoming signaling (e.g., calling party number/CLI), provided to it by the NIF, and using it (them) to retrieve location information via an associated location server/database.[20]

[20] 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 location information associated with the emergency call.

The location information is provided to the NIF for use in determining the route for the emergency call, and for populating fields/headers in 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 "Additional Data Associated with a Call" data structure.

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 will be provided in a future edition of this document.

7.1.1 Protocol Interworking Function (PIF)

To receive emergency calls from legacy originating networks, the Legacy Network Gateway is expected to SS7 trunking arrangements. Flexibility is required to accommodate different implementations for each type of interface.

7.1.1.1 SS7 Interface

When a wireline end office or MSC determines that a 1-1-2 call is to be generated, it will generate and pass some Message Transfer Part (MTP)-level information, along with Integrated Services Digital Network User Part (ISUP) information, in an SS7 Initial Address Message (IAM) to the Legacy Network Gateway. Therefore, the PIF component of the Legacy Network Gateway shall be capable of receiving and processing an SS7 ISUP IAM.

Further details related to ISUP message structure can be found in ITU-T Q.763, Q.764 and Q.767, Specifications of Signalling System No. 7 - ISDN user part.

7.1.1.1.1 SS7 Message Transfer Part (MTP) Signaling for 1-1-2 Call Setup

The wireline end office/MSC will be responsible for generating information that will be populated in an MTP message signal unit (MSU), which carries the User Part data, in this case, the ISUP IAM. The Service Information Octet (SIO) portion of an MSU sent to the Legacy Network Gateway during call set up shall be formatted as per ITU-T Q.704, Specifications of Signalling System No. 7 - Message Transfer Part, Signalling network functions and messages, Section 14.2.

The Sub-Service field in the SOI will indicate that the message is a national network message and may identify the MTP message priority. In the case of IAMs related to 1-1-2 calls, the message priority will have the value "1" (where priority 3 is the highest priority assigned to SS7 messages).[21] Therefore, the PIF component of the Legacy Network Gateway shall be capable of receiving and processing an IAM that contains MTP information that includes an SOI that contains the following information:

- The Sub-Service field shall indicate that the message is a national network message; and
- The Sub-Service field may indicate that the message priority has a value of "1".

Further details related to MTP message structure can be found in ITU-T Q.703 and Q.704, Specifications of Signalling System No. 7 – Message transfer part (MTP), Signalling link and Signalling network functions and messages, respectively.

7.1.1.1.2 SS7 ISUP Signaling for 1-1-2 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 Q.763, Signalling System No. 7 – ISDN user part formats and codes, Table 32, pages 103 and 104.

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 33 of Q.763, and generating a Release Complete Message (RLC) formatted as described in Table 34 of Q.763 in response. The PIF component of the Legacy Network Gateway will also generate a SIP BYE message toward the NIF, as described in Section 6.1.1.2.

The PIF component of the Legacy Network Gateway shall be capable of receiving and processing ISUP circuit group supervision messages sent by wireline end offices and MSCs (e.g., Blocking, Blocking Acknowledgement). The PIF component shall

[21] 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.

follow the procedures described in Q.763, Table 39, and Clauses 3.13 and 3.43, and Q.764, Sections 2.8.1, 2.8.2, 2.8.2.1, 2.8.2.2 and 2.8.2.3 for processing those messages.

The User Service Information parameter in the IAM shall indicate the following in the Bearer Capability Information Element: ITU-T standardised coding; 'speech' information transfer capability; circuit mode; and 64kbit/s information transfer rate.

7.1.1.2 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 ITU-T Q.1912.5, to generate a SIP INVITE message based on incoming SS7 signalling, and pass that INVITE message to the NIF component of the Legacy Network Gateway.

The SIP INVITE generated by the PIF will consist of the following information:

- A Request-URI that contains the information signalled in the SS7 Called Party Number parameter (per Q.1912.5).
- A To header that contains the information signaled in the SS7 Called Party Number parameter (per Q.1912.5).
- A From header that contains the information signaled in an SS7 Calling Party Number (CLI) parameter.
- A P-Asserted-Identity (PAI) header that is populated with the information contained in the SS7 Calling Party Number parameter (per Q.1912.5). In addition, the PAI header will also contain the content of the SS7 Calling Party's Category (CPC) parameter, if present in the received SS7 Initial Address Message (IAM), (per draft-patel-dispatch-cpc-oli-parameter-02).
- 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.
- A Via header that is populated with the element identifier for the Legacy Network Gateway.
- An SDP offer that includes the G.711 code.

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 Q.763, Signalling System No. 7 – ISDN user part formats and codes, Table 21, Page 97, 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 Q.763, Signalling System No. 7 – ISDN user part formats and codes, Table 22, Page 98. 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 Q.764, Signalling System No. 7 – ISDN user part signalling procedures, Section 2.1.7, Page 21 and the formatting as described in Q.763, Signalling System No. 7 – ISDN user part formats and codes, Table 22, Page 98. Specifically, in relation to the format of the ANM, the Called Party's Status indicator (Bit DC) of the Backward Call Indicators parameter will be set to "00" indicating "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."

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 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. 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, and 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.

7.1.2 Specific Interwork Function (NIF)

7.1.2.1 1.1.2.1 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 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. The NIF will make this determination based on the coding of the CPC parameter in the PAI 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) 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 an E.164 number is received in incoming signaling as the Calling Party Number (CPN)/CLI (i.e., the URI in the From and PAI headers of the INVITE message received from the PIF contains an E.164 number, i.e., CPN/CLI), the NIF will pass this number to the LIF to use in retrieving the location for the call.[22]

If the NIF determines (based on the CPC parameter in the PAI header or the trunk group information in the Contact header) that the incoming call is a legacy wireless emergency call, and a callback number (e.g., Mobile Directory Number [MDN]) is received in incoming signaling, the NIF will send that number to the LIF since it is required to uniquely identify the call.

(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 includes the location information provided by the LIF and an appropriate service URN (e.g., urn:service:sos), following the procedures described in Section 5.5.

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 an additional data structure [144] with information about the call, along with a URI pointing to the database where the additional 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 database that

[22] 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.

may be maintained at the NIF or elsewhere if maintained by the 1-1-2 Authority. The NIF will include the reference URI in the Call-Info header of the INVITE message sent to the ESRP.

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 callback information received from the LIF component, and the reference URI for the additional data structure generated by the NIF. 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 "112"
- A From header that contains the callback number (or Originating TN for legacy wireline emergency call originations) retrieved by the LIF component. If the call was originated by a non-initialized mobile caller (i.e., the callback number is of the form 112+ "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 (PAI) header that contains the callback number retrieved by the LIF component or received in incoming signaling (for legacy wireline emergency call originations**)**. If the call was originated by a non-initialized or SIMles mobile caller, the PAI header will be omitted.
- A Via header that is populated with the element identifier 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 or tel URI identifying the user to facilitate an immediate callback to the device that placed the emergency call. The Legacy Network Gateway constructs this URI, which can be anything that leads back to the Legacy Network Gateway and identifies the device which placed the call. In this case, the Contact header is expected to include the callback number that was retrieved by the LIF.
- A Supported header that contains the "geolocation" option tag.
- A Geolocation header that either:

- Points to the message body (using a "Content Identification (cid)" URI, as defined in RFC 2392) where a PIDF-LO containing the location value retrieved by the LIF is coded (see Section 7.1.3), [23] or
- Contains a location-by-reference URI.[24]

- An SDP offer that includes the G.711 codec.
- A Call Info header that contains a URI associated with the database that contains the "Additional Data Associated a Call" data structure created by the Legacy Network Gateway which, when de-referenced, would yield additional information about the call
- 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 from the ESInet in response to the SIP INVITE. If the NIF component receives a 180 Ringing message, is shall send a 180 Ringing 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.

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. If the

[23] This method will be used for wireline emergency calls and may also be used for emergency calls that originate in wireless networks that are only Phase 1 capable.

[24] This method will be used for wireless Phase 2 calls to allow the PSAP to query for initial location and location updates.

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 may also be the case for wireless emergency calls, the associated database will query an MPC/GMLC for 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), depending on the business agreements that exist between the Legacy Network Gateway provider and the data owners.

The LIF may receive one or two E.164 numbers/keys 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 the location information. If the key(s) is (are) not present in the steering data, the LIF will retrieve location data from its associated database. Specifically, if the LIF receives only a single E.164 key (i.e., CPN/ANI or ESRK) from the NIF, it will determine whether this number is contained in its steering data. If it is, it will generate an HELD (RFC 5989) or MLP (ETSI TS 102 164 V1.2.2) query to the system identified in the steering data to obtain the location information. If it is not contained in the steering data, it will retrieve the location information from its associated location database. If the LIF receives two E.164 numbers (i.e., callback number and ESRD), the LIF shall again search for these numbers in its steering data. If it finds them, it will generate an HELD or MLP query to the system identified in the steering data. If not, it will utilize internally-defined procedures/protocols to retrieve the location information from an associated location server/database. .

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 (e.g., callback number, class of service). The location value and any non-location information will be returned to the NIF.

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 location information. The LIF will generate an HELD or MLP query containing the ESRK to the MPC/GMLC and must be capable of processing A HELD or MLP response. The LIF will return the location value returned by the MPC/GMLC (which is initially expected to convey information about the location of the cell site/sector) to the NIF, along with a SIP or HELD location reference that contains the ESRK and the URI of the Legacy Network Gateway and any other non-location information, including the callback number.

If the call originated in a legacy wireless network which supports the signaling of callback number and ESRD, the LIF 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 location information. If the LIF finds steering data corresponding to the ESRD, it will generate an HELD, or MLP containing the callback number and ESRD to the MPC/GMLC and must be capable of processing an HELD or MLP response. If the legacy wireless network is only Phase I-capable, the LIF may not find steering data that corresponds to the ESRD and instead retrieve from its local database a static location value that is associated with the cell site/sector, along with any other non-location information associated with the call and return it to the NIF.

If the call originated in a wireless network which supports the signaling of callback number and ESRD, and the originating legacy wireless network is Phase II capable, the steering data in the associated location server/database associated with callback number and ESRD should include the address of the MPC/GMLC in the legacy wireless network to which an HELD or MLP query for initial/updated location information should be sent. The LIF will pass the location value returned by the MPC/GMLC (which is initially expected to convey the location of the cell site/sector) to the NIF for use in querying the ECRF. The LIF will also pass a SIP or HELD location reference that uniquely identifies the location record and the Legacy Network Gateway to the NIF, along with any other non-location information received in the E2 response.

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 de-referencing 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.

Note: This version does not describe interworking between SIP/HELD, MLP/HELD, etc. for location conveyance and location updates. This will be covered in a future edition of this document.

7.2 Legacy PSAP Gateway (LPG)

The Legacy PSAP Gateway is a signalling and media interconnection point between an ESInet and a legacy PSAP. It plays a role in the delivery of emergency calls that traverse an ESInet to get to a legacy PSAP, as well as in the transfer and alternate routing of emergency calls between legacy PSAPs and NG112 PSAPs. The Legacy PSAP Gateway supports an IP (i.e., SIP) interface towards the ESInet on one side, and a proprietary interface (usually BRI or PRI) on the other. The Legacy PSAP Gateway also includes a CLI interface, which can accept a CLI query from the legacy PSAP. The legacy PSAP controller supplies an appropriate CLI query key (i.e., "CLI") 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. If the ESInet provides a location by reference, the ALI query to the Legacy PSAP Gateway results in a dereference operation from the Legacy PSAP 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 CLI response generated by the Legacy PSAP Gateway will also contain additional information that may be obtained from a variety of sources. See Section 7.2.3 for further information.

The Legacy PSAP Gateway functional element contains three functional components, as illustrated in Figure 7-1[25]:

1. (SIP -E1/PRI/BRI according to ITU-T I.420/I.421) Protocol Interworking Function (PIF). This functional component interworks the SIP protocol to traditional ISDN, or other protocols, as appropriate for the interconnected PSAP. 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. NG1-1-2 specific Interwork Function (NIF). This functional component provides NG1-1-2-specific processing of the call signaling, which includes special handling of attached location, selection of trunk groups, and callback number mapping, etc. This functional component should be viewed as a Back-to-Back User Agent (B2BUA) in front (from the

[25] 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.

perspective of the ESInet) of the PIF. (See Section 7.2.2 for further details.)

3. Location Interwork Function (LIF). This functional component supports CLI query/response interface protocols, as well as the interworking of NG1-1-2 relevant data elements to a standardized CLI format for population in CLI response messages. (See Section 7.2.3 for further details.)

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 will be provided in a future edition of this document.

7.2.1 Protocol Interworking Function (PIF)

The PIF component of the Legacy PSAP Gateway will be responsible for interworking the SIP signalling received from the NIF component with E1-based PRI or BRI signalling sent over the interface to the destination PSAP. The PIF will also be responsible for accepting Dual Tone Multi Frequency (DTMF) signalling (e.g., that associated with transfer requests) from the legacy PSAP and sending it to the NIF component in RTP packets, per RFC 2833.

Interworking between Q.931 primary rate ISDN (EuroISDN / ETS 300 / DSS1) and SIP shall be as per ETSI TS 183 036, ISDN/SIP interworking.

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 message, 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 Contact header. Based on the information received in incoming signaling from the NIF component, the PIF component will generate E1-based PRI or BRI call signaling towards the legacy PSAP. (See Section 7.2.2.2 for further information.

7.2.1.1 E1-based, primary rate ISDN interface

The PIF component of the Legacy PSAP Gateway will be responsible for interworking the SIP signalling received from the NIF component with E1-based PRI or BRI signalling sent over the interface to the destination PSAP. The PIF will also be responsible for accepting Dual Tone Multi Frequency (DTMF) signalling (e.g., that associated with transfer requests) from the legacy PSAP and sending it to the NIF component in RTP packets, per RFC 2833.

Interworking between Q.931 primary rate ISDN (EuroISDN / ETS 300 / DSS1) and SIP shall be as per ETSI TS 183 036, ISDN/SIP interworking.

The PRI interface shall be as per ITU-T I.421, which directs the reader to the following statement: The primary rate user-network interface structures are defined in Recommendation I.412. The detailed specifications are contained in Recommendations I.431 (layer 1), I.440 and I.441 (layer 2), I.450, I.451 and I.452 (Layer 3). Thus, the signalling call control used to establish connectivity and exchange call information between the PIF and the legacy PSAP shall be as per the above specifications. Call information exchange shall include progress messages and early media/audible ringing to be returned to the calling party (via the NIF).

The PIF signals information to the PSAP CPE, based on what it receives in a SIP INVITE from the NIF component of the Legacy PSAP Gateway, which includes an indication that the call is an emergency services call. To support such functions as display or query of location and to provide callback information, the calling party's CLI digits are signalled via PRI to the legacy PSAP.

If the INVITE from the NIF contains location information in addition to callback information (i.e., a CLI), the PIF will signal the CLI and the location information in PRI signaling to the legacy PSAP. The location information shall be signalled using the user-to-user information element within the PRI signaling information. Note that the legacy PSAP will use the CLI as a location key if it needs to query for and update the location of an emergency caller. Note also that the location information signaled to the legacy PSAP by the PIF is likely to be 'phase 1' location.

7.2.1.2 Basic rate ISDN interface.

The BRI interface shall be as per ITU-T I.420, which directs the reader to the following statement: The basic user-network interface structure is defined in Recommendation I.412. The detailed specifications are contained in Recommendations I.430 (layer 1), I.440 and I.441 (layer 2), I.450, I.451 and I.452 (layer 3).

7.2.2 NG1-1-2 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 5.1. Specifically, the NIF component of the Legacy Network Gateway must be capable of receiving and processing an INVITE that includes the following information:

- Request URI = PSAP URI resolving at the gateway[26]
- Max Forwards <70
- Record Route = ESRP URI
- Route header = urn:service:sos
- From = Callback Number/Address or "Anonymous," if unavailable
- To: sip:112@vsp.com (Note: This is an example of a possible SIP URI rather than a pre-defined one.)
- P-Asserted-Identity (PAI) = the callback number/address or omitted if call is from a non-initialized mobile caller (i.e., P-Preferred-Identity containing 112 + last 7 digits of the ESN or IMEI expressed as a decimal" is present)
- P-Preferred-Identity (P-PI) = 112 + "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 (added to other Via headers present in INVITE received by the terminating ESRP)
- Contact = SIP URI or tel URI identifying the user to facilitate an immediate callback to the device that placed the emergency call
- Supported = as received by the terminating ESRP
- SDP = as received by the terminating ESRP
- Geolocation = content id URI or location reference
- Call Info = a URI which, when de-referenced, would yield additional information about the call
- History-Info = as specified in RFC 4244 (will be present if call has undergone diversion)
- Reason – as specified in RFC 3326 (will be present if call has undergone diversion).

[26] 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.

Upon receiving an INVITE message from an ESRP, the NIF component will analyze the signaled information and apply NG1-1-2-specific processing to ensure that the information delivered to the legacy PSAP is in an acceptable format.

7.2.2.1 Handling of Emergency Calls with Non-NANP Callback Information

It is possible that VoIP emergency call originations will contain callback information that is not in the form of (or easily converted to) an E.164 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 primary or basic rate ISDN 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 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 callback numbers mapped by the NIF component. The NIF must determine, based on provisioning, whether the interface to the target PSAP is a primary or basic rate ISDN 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 (that it gets from an ESRP) in the following way:

- If the incoming INVITE message contains a P-AI header, it will use the information in this header as callback information.
- If the incoming INVITE message does not contain a P-AI 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.
- If the PSAP expects callback information to be delivered, but the callback information is unavailable or is of the form 112+ "last 7 digits of the ESN or IMEI expressed as a decimal," and location information, in the form of a reference, is available, the NIF should signal the location information in the From header.

Further study is needed to determine what should be populated to signal calls originating from VoIP customers.

The NIF will obtain location information, in the form of a civic address or location metrics e.g., coordinates, from the Geolocation header of the incoming INVITE message. The NIF should send this information to the PIF in a Geolocation header in an INVITE message (and the PIF should send this, if present, to the legacy PSAP in primary rate ISDN signalling as user-to-user information).

7.2.2.2.1 INVITE Message Sent from NIF Component to PIF Component

The INVITE message sent by the NIF component to the PIF component shall be as per RFC 3261 and will contain the following information:

- Request URI = PSAP URI resolving at the gateway
- Max Forwards <70
- Record Route = ESRP URI
- Route header = urn:service:sos
- From = See Table 7-1
- To = sip:112@vsp.com (Note: This is an example of a possible SIP URI rather than a pre-defined one.)
- PAI = the callback number (i.e., the CLI) of the calling party
- Via = an identifier for the Legacy PSAP Gateway
- Supported = as received by the NIF component
- SDP = as received by the NIF component
- Geolocation = as received by the NIF component
- Call Info = 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
- A Contact header that contains the trunk group parameters that identify the outgoing trunk group to the destination PSAP, as defined in RFC 4904.

The interface between the NIF and the PIF shall conform to RFC 3261 in relation to the INVITE method and furthermore, the NIF and the PIF shall support the interchange of session progress messages such as e.g., SIP 100 Trying, SIP 200 OK, SIP 18x, and SIP BYE messages.

7.2.2.3 Support for Emergency Call Transfer

When a legacy PSAP determines that it is necessary to transfer an emergency call, it sends a SETUP signal and waits for CONNECT ACK. it 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 'SETUP, it will follow the Q.931 the signal to the NIF component of the Legacy PSAP Gateway and provide dial tone to the legacy PSAP. The NIF will 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.

Section 5.1.1.2 provides a more complete discussion of the REFER method, and Sections 4.8 and 4.9 provide detail flows describing the alternatives for supporting bridging and transfer in an i3 environment.

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 4.8. 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 4.8, 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 AdditionalPSAPData structure (which contains the AdditionalCallData and AdditionalCallerData if present in the call) to pass to the secondary PSAP as an escaped Call-Info header (as described in Section 4.8.1.3). 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 in Figure 6.

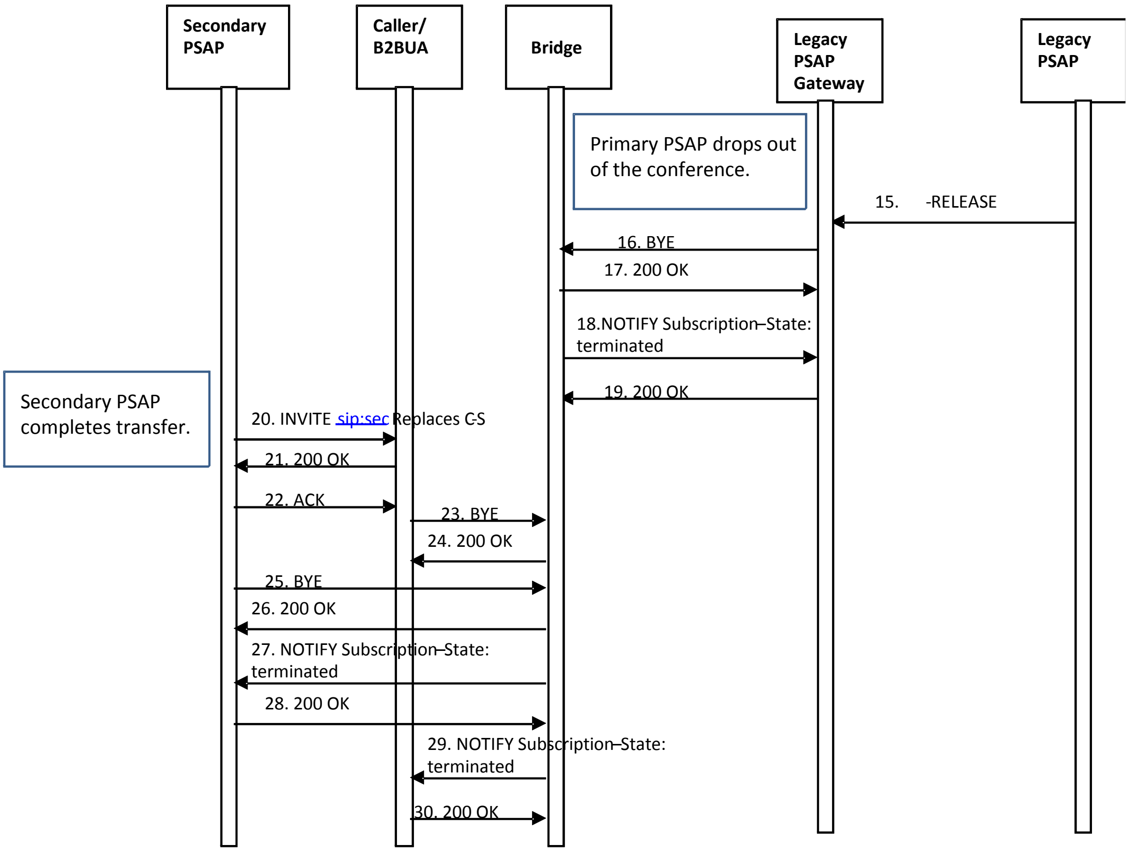

Secondary PSAP
Caller/ B2BUA
Bridge
Legacy PSAP Gateway
Legacy PSAP
Primary PSAP drops out of the conference.
15. -RELEASE
16. BYE
17. 200 OK
18.NOTIFY Subscription-State: terminated
19. 200 OK
Secondary PSAP completes transfer.
20. INVITE sip:sec Replaces CS
21. 200 OK
22. ACK
23. BYE
24. 200 OK
25. BYE
26. 200 OK
27. NOTIFY Subscription-State: terminated
28. 200 OK
29. NOTIFY Subscription-State: terminated
30. 200 OK

Figure 6: 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.

16.- When the Legacy PSAP Gateway receives the RELEASE signal, 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.

7.2.2.4 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. In an NG 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 either all channels are busy, time-out conditions in waiting queues …. Upon detecting the alternate routing request, the Legacy PSAP Gateway will return an 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.

7.2.3 Location Interwork Function (LIF)

The Legacy PSAP Gateway must support an ALI interface which can accept an ALI query from the legacy PSAP and return location information. 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 E.164 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. The Legacy PSAP Gateway can also generate an appropriate Class of Service for the call. 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.

The Legacy PSAP Gateway will need to access "Additional Data" structures to populate other fields in the ALI response. To do this, the Legacy PSAP Gateway will need to support the HTTP GET method described in IETF RFC 2616. The Legacy PSAP Gateway will use the information contained in the Call Info header of the received INVITE to identify the address of the target subscriber database to which the GET will be directed. The Legacy PSAP Gateway shall be capable of receiving and processing the XML-formatted data in the response from the subscriber data, and using it to populate the appropriate fields of the ALI response message.

8 Data Associated with call/caller/location/PSAP

IP-based emergency services offer a much richer communication exchange and thereby better situational awareness for call takers. The richness comes in various forms, including multi-media communication capabilities (via voice, video, instant messaging, and real-time text), but also via more extensive flow of information. Sharing information between various actors can enable more intelligent decision making and therefore better response in case of an emergency. A prerequisite is to offer the technical capabilities to let call takers gain access to such information stored elsewhere (assuming that they are authorized to access it).

In general, there are four types of data exchanged:

- **Data associated with a Call**: A lot of information is carried in the call setup procedure itself (as part of the SIP headers as well as in the body of the SIP message, e.g., for example supported capabilities of the device). This also includes information about the emergency caller's identity. This information is part of the SIP protocol exchange itself and discussed throughout the document.
- **Data associated with a Location**: Location information is available via the PIDF-LO element, which includes civic and geospatial location, information about the entity that provided the data, information about how the location was obtained (as expressed by the <method> element, see Section 2.2.3 of [RFC4119], and the values registered in http://www.iana.org/assignments/method-tokens/method-tokens.xml), and which entity or organization supplied location information (beyond the domain information that can be inferred from a signing certificate) available via the <provided-by> element.
- **Data associated with a Caller**: This is personal data about a caller, including medical information.
- **Data associated with a PSAP**: When a PSAP handles a call it develops information about the call, which must be passed to subsequent PSAPs, dispatchers and/or responders.

Additional Data is defined as data that is associated with a call, a caller, a location or a PSAP. A description about the data structures can be found in [144].

Additional Data is either attached to the SIP signaling itself (as an additional payload in the body) or a URI is attached to the call. In the former case we are technically talking about using content indirection (CID) to indicate that the data is carried within the body of the SIP message. In the latter case the URI is a pointer to the data structure in a database and needs to be dereferencing with an HTTPS GET request (with fallback to HTTP, if appropriate). To ensure proper authentication and authorization ESInet elements retrieving this data using the provided URI need to use credentials traceable to the PCA, which must be accepted by the entity holding the data.

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.

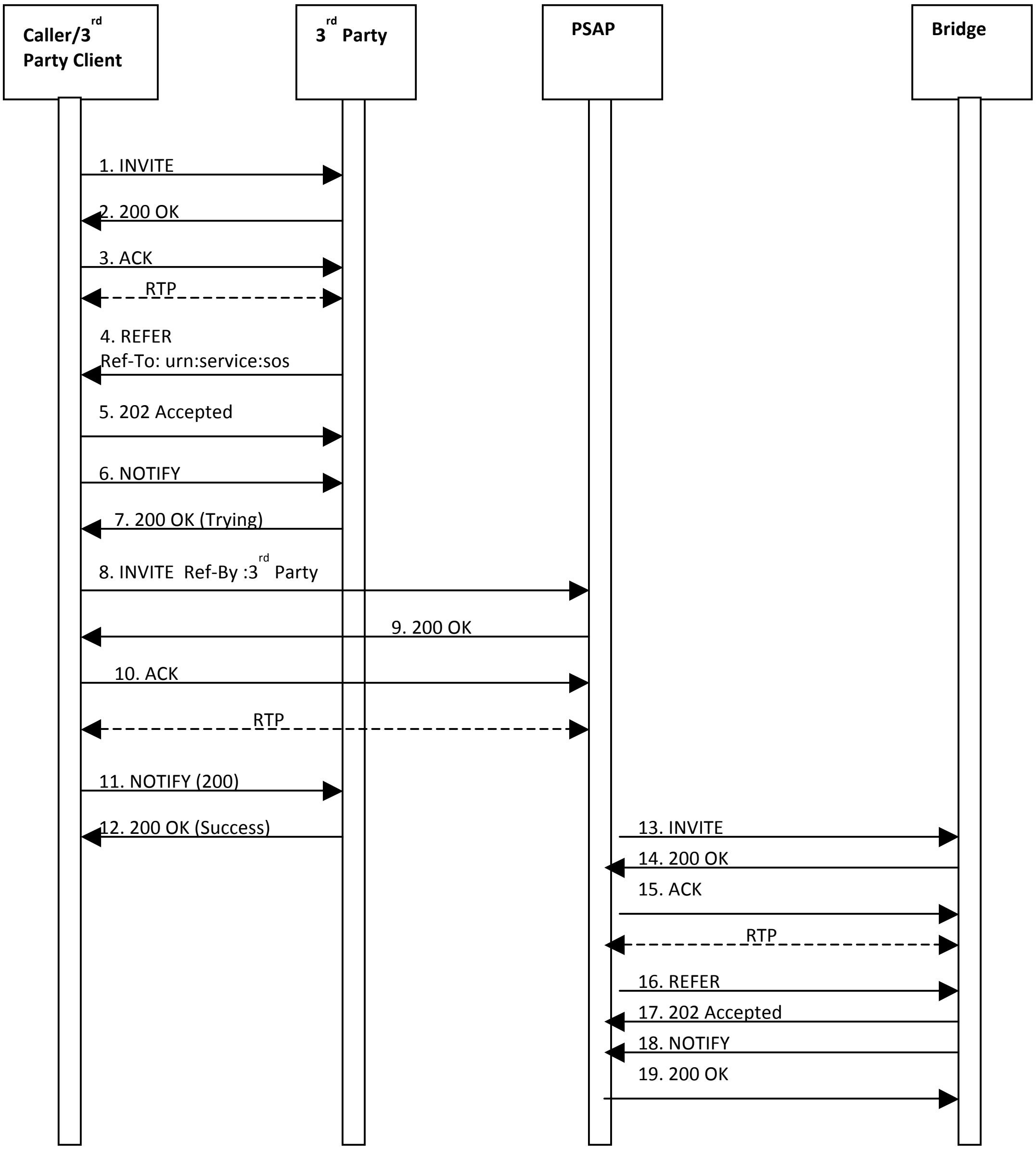
The caller is assumed to have a two-way SIP call between the caller and the call agent. Service providers who do not use SIP between the call and the call agent may use a gateway to interwork the call signaling from the caller to SIP, and must similarly use a gateway to interwork the call agent signaling to SIP. In such cases, the following signaling description applies, even though the call starts without a SIP call between the caller and call agent.

In order to save time in emergency call connection when the operator of the caller has information on what call center to invoke, the operaqtor of the caller can handle the three party call setup, so that a call leg is set up with the PSAP and another with the call agent simultaneously.

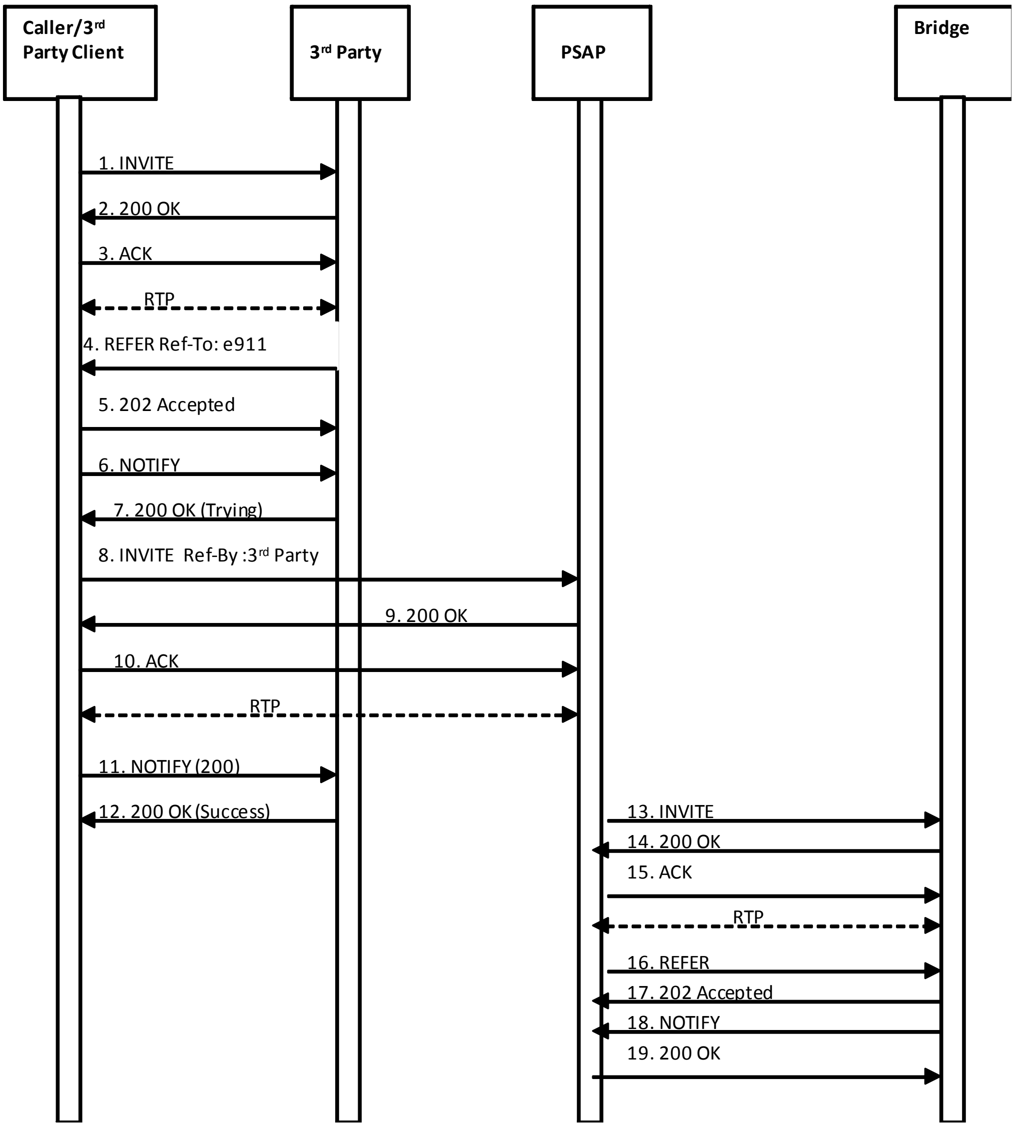
A relay service for trranslation between sign language or text and speech is a typical such call centre.

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 calls 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.



Caller/3rd Party Client
3rd Party
PSAP
Bridge
1. INVITE
2. 200 OK
3. ACK
RTP
4. REFER
Ref-To: urn:service:sos
5. 202 Accepted
6. NOTIFY
7. 200 OK (Trying)
8. INVITE Ref-By :3rd Party
9. 200 OK
10. ACK
RTP
11. NOTIFY (200)
12. 200 OK (Success)
13. INVITE
14. 200 OK
15. ACK
RTP
16. REFER
17. 202 Accepted
18. NOTIFY
19. 200 OK



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 112 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

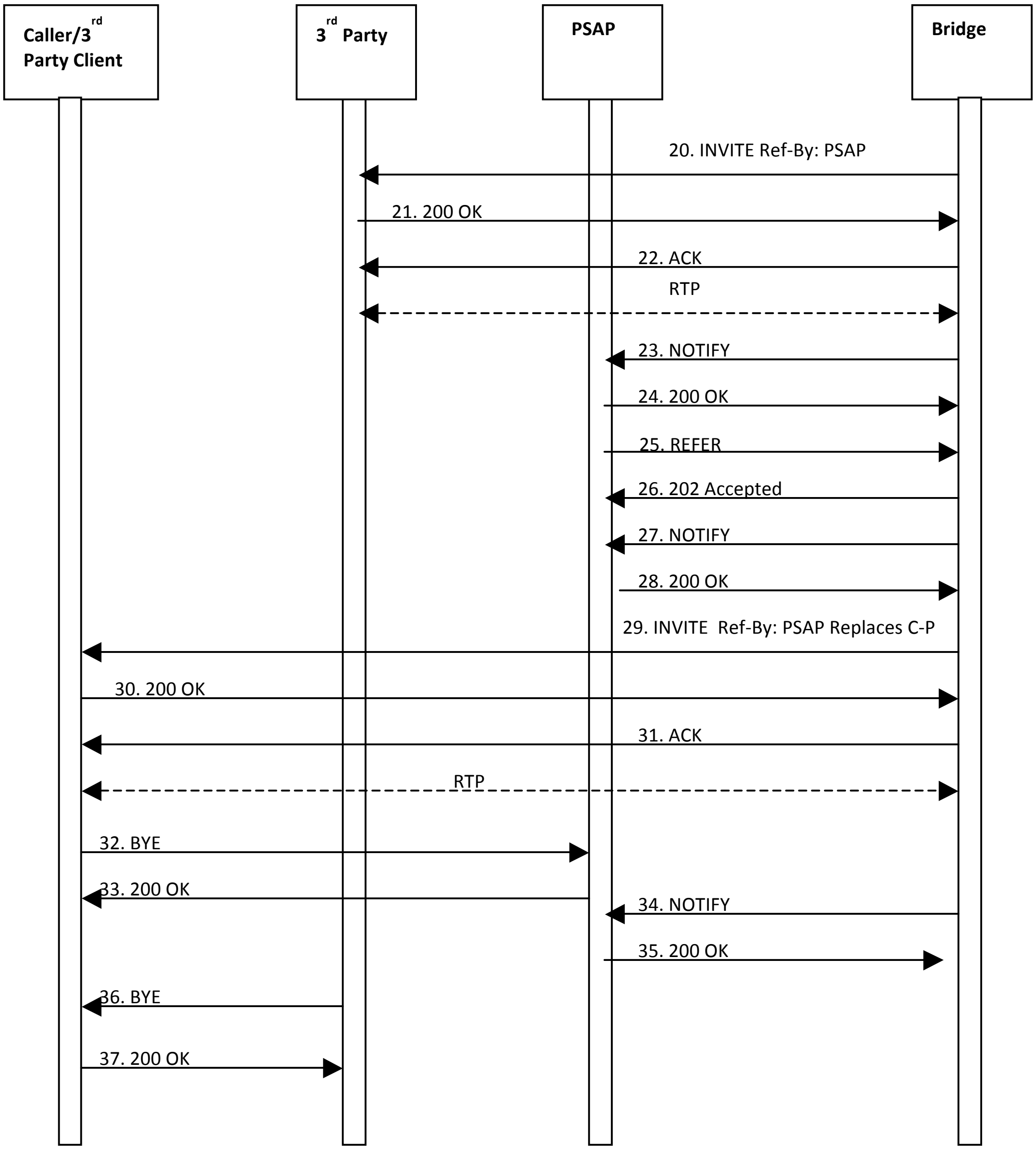
the call agent includes an AdditionalCallData URI in an escaped Call-Info header in the REFER.

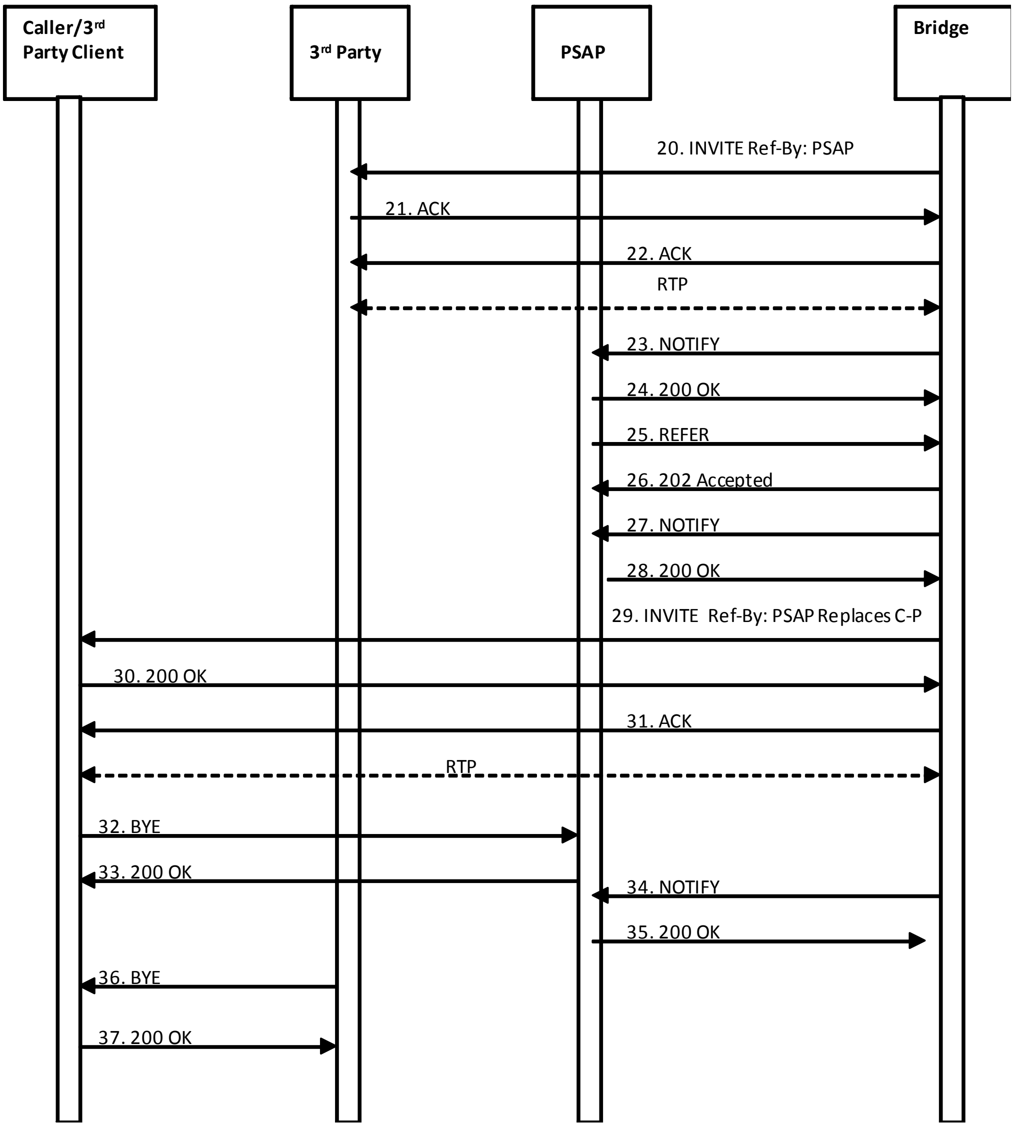
5. The caller/3rd party client responds by returning a 202 Accepted message to the 3rd party call agent.
6. The caller/3rd party client also returns a NOTIFY message, indicating the subscription state of the REFER request (i.e., active).
7. The 3rd party call agent returns a 200 OK message in response 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 112 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 AdditionalCallData URI that it received in the escaped Call-Info header 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


Caller/3rd Party Client
3rd Party
PSAP
Bridge
20. INVITE Ref-By: PSAP
21. 200 OK
22. ACK
RTP
23. NOTIFY
24. 200 OK
25. REFER
26. 202 Accepted
27. NOTIFY
28. 200 OK
29. INVITE Ref-By: PSAP Replaces C-P
30. 200 OK
31. ACK
RTP
32. BYE
33. 200 OK
34. NOTIFY
35. 200 OK
36. BYE
37. 200 OK



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 an 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 the Additional Call Data, 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 a disconnect of the original session between them (step 36).

10 Integration with non-SIP-based Systems

Many Internet and telecommunications providers, equipment manufacturers and software providers have focused their attention on SIP-based communication protocols. As part of that industry effort many of the emergency services extensions defined in different standards developing organizations are available for SIP only. This document makes use of these standards.

However, SIP is not the only IP-based protocol that is deployed today. For example, in the area of instant messaging the Extensible Messaging and Presence Protocol (*XMPP*) has become fairly popular. For voice and video communication proprietary protocols have been utilized, such as Skype. There are also various applications available for smart phones and Internet tablets that use proprietary protocols. The most recent development is related to standardization efforts for real-time communication in Web browsers, called RTCWEB. RTCWEB makes use of new JavaScript APIs to allow browsers to use multi-media communication integrated into regular Web applications. These Web applications may not even need to look like regular Webpages but may also include smart phone applications utilizing HTML5 technology.

The Internet allows everyone to develop their own favorite communication protocol and to deploy it.

Quite naturally, the question arises on how these systems can be integrated into the emergency services architecture outlined in this document. Does this document need to get updated every time a new communication protocol emerges? Do emergency services networks need to be continuously updated to keep up-to-date with new Internet application protocols that are enjoyed by so many end users?

Fortunately, emergency services networks do not need to be updated due to the new arrival of new smart phone application or Internet protocol. Figure 7 illustrates how the integration of these applications is envisioned.

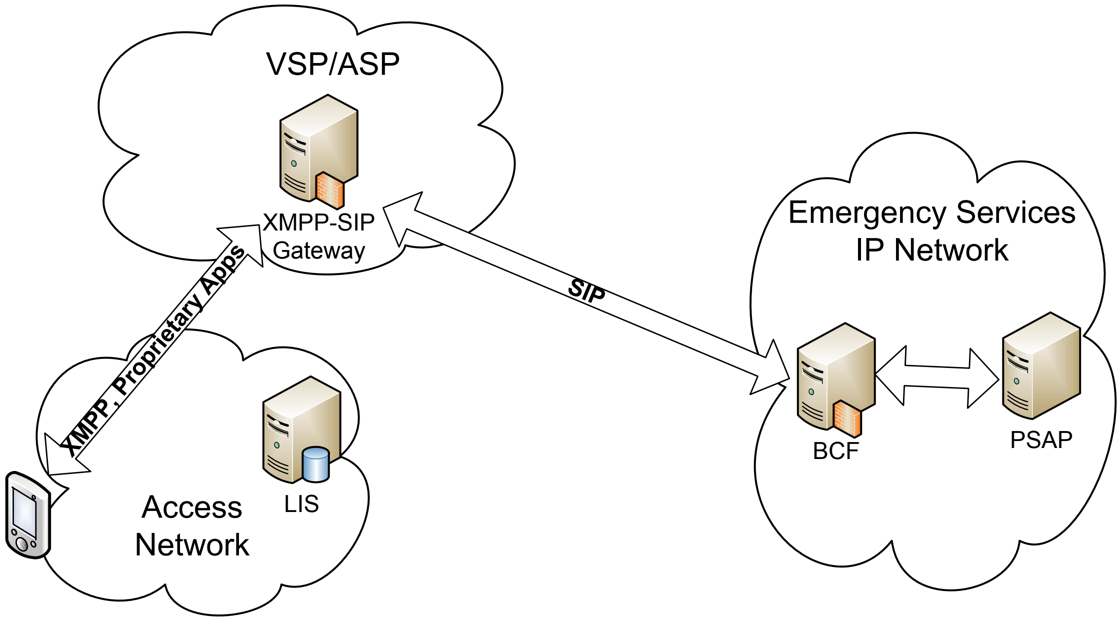


Figure 7: Interworking.

End users equipped with the end devices may use a protocol of choice with their voice / application service providers. For example, they may use XMPP for instant messaging, they may use RTCWEB with their Web browsers, or any other proprietary application development. If there is, however, the need to interwork with the emergency services networks then these VSPs/ASPs translate these protocol messages into SIP as described in this specification.

There are two major advantages using this architecture:

1. VSPs and ASPs can innovate at their own speed and offer features to their customers without having to worry about the status of emergency service standardization for the technical protocol mechanisms they use.
2. Emergency authorities do not need to update their software and hardware continuously to stay up-to-date with the latest Internet protocol developments.

There are, however, drawbacks of this approach as well.

1. First, the burden to interoperate with emergency infrastructure is with the ASP/VSP since they have to develop additional software to translate their proprietary protocol messages to SIP for interworking.
2. Second, there may be loss in functionality since proprietary developments may provide additional features not yet standardized for SIP-based emergency services.

To avoid the drawbacks listed above we recommend that application developers who target the emergency services sector with their developments specifically to make use of the available standards. There are also many software libraries available that can be re-used to speed-up their development.

11 Organizational Descriptions

This section provides a summary of the organizations described in this document.

1. **Certificate Authority**

A certificate authority (CA) that issues certificates to different entities in the emergency services networks has to be created or the services of an existing CA have to be re-used. This enables proper authentication, and builds the foundation for authorization. The overall level of security will be substantially improved as a consequence.

Since this document assumes a public key infrastructure the use of such a certificate authority for usage with emergency services organizations is needed. Note that a CA is responsible for managing the entire lifecycle of certificates from the creation to termination or revocation.

2. **European, National, and Regional Authorities**

Applicable laws, regulations and rules may need to be enhanced to support NG112 system deployment. This is particularly true to provide the necessary provisions to require access network providers to share IP location information and VSPs/ASPs to transmit emergency calls to emergency services authorities.

3. **Public Safety Computer Emergency Response Team (CERT)**

To react to security breaches and other incidents the creation of a Public Safety Computer Emergency Response Team (CERT) is anticipated, and all stakeholders must arrange to receive alerts from the CERT and to respond. It is essential that all 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 mitigate such attacks.

4. **European Emergency Services Registry Service (ERS):**

The European Emergency Services Registry Service (ERS) is a Web site that contains protocol parameters and has to be established. This registry will be published within EENA's website. The location of the ERS may be changed in the future.

5. **112 Authorities**

The national/regional/local authorities are responsible for overall operation of, and the data for the 112 system:

- It is in charge of operating the state/regional/local Emergency Service Routing Proxy (ESRP). A terminating ESRP may be operated by a PSAP. The ESRP for non-originating ESRPs must supply a ruleset for the upstream ESRP.
- Should provide a state/regional/local Emergency Call Routing Function (ECRF)
- Is responsible for maintaining the integrity of the data housed in the ECRF systems.
- 112 authorities will also provide input to the definition of policies, which dictates the granularity of the routing decisions returned by the ECRF (i.e., ESRP URIs vs. PSAP URIs).
- 112 authorities provide data about PSAP boundaries. This data is, for example, using in LoST servers and influences routing decisions.
- In case of gaps and overlaps in these boundaries, 112 authorities are responsible to address these issues.
- ECRF must be accessible from the Internet so that VSPs and ASPs can route emergency calls to them.
- The source SIF may be provided by 112 authorities or other government agencies with GIS responsibility (e.g., a county mapping agency and/or responders who define their own service areas).
- 112 authorities are responsible to provide an authoritative GIS database containing only valid civic addresses. This information is used for the location validation.
- 112 authorities have to decide about the setup, and operation of the ESInet as well as PSAPs and other IT infrastructure equipment necessary to operate the IP network, interconnection points, and call routing equipment.

12 Test Calls

PSAPs must implement the test function described in [59]. As the function is designed to test if a 1-1-2 call was placed from the test-initiating device, the test mechanism should mimic the entire actual 1-1-2 call path as closely as practical. The test mechanism is completely automatic, with no manual intervention required.

An INVITE message with the Service URN (found in a Route header) of “urn:service:sos.test” 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 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 [137] 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.

13 Parameter Registries

This document requires several registries to be created and those populated with initial values. The entity that creates these values and makes them available over the Web within EENA is called the European Emergency Services Registry Service (ERS). ERS needs to ensure that the policies associated with the parameter registries are followed to avoid inconsistency in the registry. The URN "ees" is established with [176].

13.1 elementState Registry

The elementState event returns an enumerated value of the current state of an agency or element as defined in Section 5.6.2. A registry is needed to enumerate the possible values returned.

13.1.1 Name

The name of this registry is elementState.

13.1.2 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.

13.1.3 Management Policy

A Technical Document required to add a new entry into the registry.

13.1.4 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 Technical Standard that defines the label.

13.1.5 Initial Values

The initial value and purposes of the registry are found in Section 5.6.2.

13.2 serviceState Registry

The serviceState event returns an enumerated value of the current state of a service as defined in Section 5.6.3. A registry is needed to enumerate the possible values returned.

13.2.1 Name

The name of this registry is serviceState

13.2.2 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.

13.2.3 Management Policy

A Technical Document is required to add a new entry into the registry.

13.2.4 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 Technical Document that defines the label.

13.2.5 Initial Values

The initial value and purposes of the registry are found in Section 5.6.3.

13.3 securityPosture Registry

The SecurityPosture event returns an enumerated value of the current security posture of an agency or element as defined in Section 5.6.1. A registry is needed to enumerate the possible values returned.

13.3.1 Name

The name of this registry is securityPosture.

13.3.2 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.

13.3.3 Management Policy

A ERS Technical Document is required to add a new entry into the registry.

13.3.4Content

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 ERS Technical Document that defines the label.

13.3.5Initial Values

The initial value and purposes of the registry are found in Section 5.6.1. The reference is this document.

13.4 ExternalEventCodes 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 EENA as outlined in Section 5.1.10.

13.4.1Name

The name of this registry is ExternalEventCode.

13.4.2Information 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.

13.4.3Management 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.

13.4.4Content

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 requesting the entry.

13.4.5Initial Values

The registry should have the following entries:

Value	**Purpose**	**Reference**
VEDS	A message from an automatic vehicle alert system containing a VEDS dataset	<insert reference to this document>
BISACS	A message from an intelligent building or a building central alarm monitoring service containing a BISACS alert message	<insert reference to this document>

13.5 EsrpNotifyEventCodes Registry

CAP messages are used for events sent to, and within an ESInet. CAP messages have an <event code> tag. For use the ESRPnotify event, 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 as outlined in Section 4.3.1.5

13.5.1Name

The name of this registry is EsrpNotifyEventCode.

13.5.2Information 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.

13.5.3Management 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.

13.5.4Content

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 who created the entry.

13.5.5Initial Values

The registry should have the following entries:

Value	Purpose	Category	Reference

13.6 RouteCause Registry

13.6.1Name

The name of this registry is RouteCause.

13.6.2Information 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.

13.6.3Management 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 differentiateable 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.

13.6.4Content

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 that created the entry.

13.6.5 Initial Values

The registry should have the following entries:

Value	Code	Text	Reference
NormalNextHop	200	Normal Next Hop	<insert reference to this document>
TimeOfDay	401	Time of Day	<insert reference to this document>
	402		<insert reference to this document>

13.7 LogEvent Registry

Log entries have a LogEvent, which specifies what kind of log record the entry contains. Log entries are defined in Section 4.13.1.1.

13.7.1Name

The name of this registry is LogEvent.

13.7.2Information 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.

13.7.3Management Policy

An ERS Technical Document is required to add a new entry into the registry

13.7.4Content

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 Technical Document that defines the LogEvent.

13.7.5Initial Values

The initial value and purposes of the registry are found in Section 4.13.1.1. The reference is this document.

13.8 AgencyRoles Registry

Agencies are classified by a role in the ESInet.

13.8.1Name

The name of this registry is AgencyRoles.

13.8.2Information required to create a new value

A new entry to AgencyRole requires a definition of the role, and must be suitably explicit to differentiate the role from existing roles.

13.8.3Management Policy

An ERS Technical Document is required to add a new entry into the registry.

13.8.4Content

This registry contains:

- The UTF-8 "role" of the entry
- A reference (URI) to the EENA Document that defines the role.

13.8.5Initial Values

To be defined in further versions of this document.

13.9 AgentRoles Registry

Agents authenticate to the ESInet in one or more roles. The roles are defined in an OID to be referenced in a future edition of this document.

13.9.1Name

The name of this registry is AgentRoles.

13.9.2Information 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.

13.9.3Management Policy

A technical Document is required to add a new entry into the registry. Normally, this will be a revision to a specific OID (to be created) that defines all NG112 agent roles.

13.9.4Content

This registry contains:

- The UTF-8 "role" of the entry
- A reference (URI) to the Technical Document that defines the role.

13.9.5Initial Values

To be defined in further versions of this document.

14 References

Note that this version of the document contains many references to documents that are works in progress at the IETF and other organizations. As such this document may be revised as these references stabilize.

1. [deleted]
2. EENA Terminology Operations Document, EENA 1.1.4
3. [deleted]
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. Cuellar 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 Event, 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, draft-ietf-ecrit-phonebcp (work in progress)

60. Location-to-URL Mapping Architecture and Framework, H. Schulzrinne, Internet Engineering Task Force, RFC5582

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, J. Urpalainen, Internet Engineering Task Force, RFC 6501

64. IP Multimedia Subsystem (IMS) emergency sessions, 3rd Generation Partnership Project, 3GPP TS 23.167

65. [deleted]

66. [deleted]

67. [deleted]

68. [deleted]

69. [deleted]

70. [deleted]

71. [deleted]

72. [deleted]

73. [deleted]

74. [deleted]

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, H. Tschofenig, H. Schulzrinne, M. Thomson, Internet Engineering Task Force, RFC 6753

79. Session Initiation Protocol (SIP) Overload Control, V. Gurbani, V. Hilt, H. Schulzrinne, Internet Engineering Task Force, draft-ietf-soc-overload-control (work in progress)

80. [deleted]

81. [deleted]

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. [deleted]

89. [deleted]

90. (Extensible Markup Language) XML-Signature Syntax and Processing, D. Eastlake, J. Reagle, D. Solo, Internet Engineering Task Force, RFC 3275

91. IETF Working Group on System for Cross-domain Identity Management, http://datatracker.ietf.org/wg/scim/charter/.

92. [deleted]

93. RTP Control Protocol Extended Reports (RTCP XR), T. Friedman ed., Internet Engineering Task Force, RFC 3611

94. [deleted]

95. Common Alerting Protocol V1.0, A. Botterell, Organization for the Advancement of Structured Information Standards (OASIS), oasis-200402-cap-core-1.0

96. [deleted]

97. [deleted]

98. [deleted]

99. An INVITE-Initiated Dialog Event Package for the Session Initiation Protocol (SIP), J. Rosenberg, H. Schulzrinne, R. Mahy, Internet Engineering Task Force, RFC 4235

100. 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

101. [deleted]

102. NENA Technical Information Document Network/System Access Security, National Emergency Number Association, NENA 04-503

103. Filtering Location Notifications in the Session Initiation Protocol (SIP), R. Mahy, B. Rosen, H. Tschofenig, Internet Engineering Task Force, RFC 6447

104. Use of Device Identity in HTTP-Enabled Location Delivery (HELD) J. Winterbottom, M. Thomson, H. Tschofenig, R. Barnes, Internet Engineering Task Force, RFC 6155

105. [deleted]

106. Domain Names -- Concepts And Facilities, P. Mockapetris, Internet Engineering Task Force, STD13

107. A DNS RR for specifying the location of services (DNS SRV), A. Gulbrandsen, P. Vixie, L. Esibov, Internet Engineering Task Force, RFC2782

108. SIPconnect Technical Recommendation V1.0, C. Sibley, C. Gatch, SIPforum, sf-adopted-twg-IP_PBX_SP_Interop-sibley-sipconnect

109. [deleted]

110. Interworking between the Session Initiation Protocol (SIP) and the Extensible Messaging and Presence Protocol (XMPP): Instant Messaging, P. Saint-Andre, Internet Engineering Task Force, draft-saintandre-sip-xmpp-im (work in progress)

111. [deleted]

112. Synchronizing Service Boundaries and <mapping> Elements Based on the Location-to-Service Translation (LoST) Protocol, H. Schulzrinne, H. Tschofenig, Internet Engineering Task Force, RFC 6739

113. Session Initiation Protocol (SIP) Event Notification Extension for Notification Rate Control, A. Niemi, K. Kiss, S. Loreto, Internet Engineering Task Force, RFC 6446

114. Design Considerations for Session Initiation Protocol (SIP) Overload Control, V. Hilt, E. Noel, C. Shen, A. Abdelai, Internet Engineering Task Force, RFC 6357

115. [deleted]

116. Session Traversal Utilities for NAT (STUN), J. Rosenberg, R. Mahy, P. Matthews, D. Wing, Internet Engineering Task Force, RFC 5389

117. Framework for Real-Time Text over IP Using the Session Initiation Protocol (SIP), A. van Wijk, G. Gybels, Internet Engineering Task Force, RFC 5194

118. RTP Payload for Text Conversation, G. Hellstrom, P. Jones, Internet Engineering Task Force, RFC 4103

119. Framework for Transcoding with the Session Initiation Protocol (SIP), G. Camarillo, Internet Engineering Task Force, RFC 5369

120. Indication of Message Composition for Instant Messaging, H. Schulzrinne, Internet Engineering Task Force, RFC 3994

121. The Message Session Relay Protocol (MSRP), B. Campbell, R. Mahy, C. Jennings, Internet Engineering Task Force, RFC 4975

122. Relay Extensions for the Message Session Relay Protocol (MSRP), C. Jennings, R. Mahy, A.B. Roach, Internet Engineering Task Force, RFC 4976

123. Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types, N. Freed, N. Borenstein, Internet Engineering Task Force, RFC 2046

124. vCard MIME Directory Profile, F. Dawson, T. Howes, Internet Engineering Task Force, RFC 2426

125. The Secure Real-time Transport Protocol (SRTP), M. Baugher, et. al., Internet Engineering Task Force, RFC 3711

126. Session Description Protocol (SDP) Security Descriptions for Media Streams, F. Andreasen, M. Baugher, D. Wing, Internet Engineering Task Force, RFC 4568

127. [deleted]

128. 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

129. Filtering Location Notifications in the Session Initiation Protocol (SIP), R. Mahy, B. Rosen, H. Tschofenig, Internet Engineering Task Force, RFC 6447

130. [deleted]

131. [deleted]

132. [deleted]

133. [deleted]

134. Voice Extensible Markup Language (VoiceXML) Version 2.0, S. McGlashan et. al., World Wide Web Consortium, REC-voicexml20-20040316

135. Real Time Streaming Protocol (RTSP), H. Shulzrinne, A. Rao, R. Lanphier, Internet Engineering Task Force, RFC 2326

136. The Session Description Protocol (SDP) Label Attribute, O. Levin, G. Camarillo, Internet Engineering Task Force, RFC 4574

137. An Extension to the Session Description Protocol (SDP) for Media Loopback, H. Kaplan et al., Internet Engineering Task Force, draft-ietf-mmusic-media-loopback (work in progress)

138. "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.

139. "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.

140. "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.

141. "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)", draft-ietf-avt-rtp-evrc-nw (work in progress).

142. [deleted]

143. [deleted]

144. "Additional Data related to a Call for Emergency Call Purposes", B. Rosen, H. Tschofenig, R. Marshall, Internet Engineering Task Force, draft-ietf-ecrit-additional-data (work in progress)

145. "RObust Header Compression (ROHC): Framework and four profiles: RTP, UDP, ESP, and uncompressed", C. Bormann et. al., Internet Engineering Task Force, RFC 3095

146. "Geolocation Policy: A Document Format for Expressing Privacy Preferences for Location Information", H. Schulzrinne, H. Tschofenig et. al, Internet Engineering Task Force, draft-ietf-geopriv-policy (work in progress)

147. "Common Policy: A Document Format for Expressing Privacy Preferences", H. Schulzrinne et. al., Internet Engineering Task Force, RFC 4745

148. "Detailed Functional and Interface Specification for the NENA i3 Solution – Stage 3", National Emergency Number Association (NENA) VoIP/Packet Technical Committee Long Term Definition Working Group, NENA i3

149. Operational and Interworking Requirements for DCEs operating in the Text Telephone Mode. ITU-T Recommendation V.18

150. "XML Schema for media control." R.Even et. al. , Internet Engineering Task Force, RFC 5168

151. "Codec Control Messages in the RTP Audio Visual Profile with Feedback." S.Wenger et. al. Internet Engineering Task Force, RFC 5104.

152. ETSI EN 300-008-1 SS7 MTP, ETSI

153. ETSI EG 202 320 Duplex Universal Text and Speech, ETSI

154. H. Schulzrinne, H. Tschofenig, C. Holmberg, M. Patel, "Public Safety Answering Point (PSAP) Callback", draft-ietf-ecrit-psap-callback, (work in progress).

155. D. Wing, S. Niccolini, M. Stiemerling, H. Tschofenig, "Spam Score for SIP", draft-wing-sipping-spam-score-02, (work in progress), Feb. 2008.

156. R. Barnes, M. Lepinski, A. Cooper, J. Morris, H. Tschofenig, H. Schulzrinne, "An Architecture for Location and Location Privacy in Internet Applications", RFC 6280, July 2011.

157. J. Polk, "IANA Registering a SIP Resource Priority Header Field Namespace for Local Emergency Communications", draft-ietf-ecrit-local-emergency-rph-namespace-04, (work in progress), March 2010.

158. M. Thomson, J. Winterbottom, "Using Device-provided Location-Related Measurements in Location Configuration Protocols", draft-ietf-geopriv-held-measurements-04, (work in progress), October 2011.

159. FBI. Don't Make the Call - The New Phenomenon of 'Swatting', February 2008, available at http://www.fbi.gov/news/stories/2008/february/swatting020408

160. M. Thomson, J. Winterbottom, "Discovering the Local Location Information Server (LIS)", RFC 5986, September 2010

161. E. Rescorla, "HTTP Over TLS", RFC 2818, May 2000

162. D. Atkins, R. Austein, "Threat Analysis of the Domain Name System (DNS)", RFC 3833, August 2004

163. L. Daigle and A. Newton. Domain-Based Application Service Location Using SRV RRs and the Dynamic Delegation Discovery Service (DDDS), RFC 3958, January 2005

164. L. Daigle. Domain-Based Application Service Location Using URIs and the Dynamic Delegation Discovery Service (DDDS), RFC 4848, April 2007

165. C. Jennings, J. Peterson, and M. Watson. Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks, RFC 3325, November 2002

166. J. Peterson and C. Jennings. Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP), RFC 4474, August 2006

167. F. Andreasen, M. Baugher, and D. Wing. Session Description Protocol (SDP) Security Descriptions for Media Streams, RFC 4568, July 2006

168. D. Wing, S. Fries, H. Tschofenig, and F. Audet. Requirements and Analysis of Media Security Management Protocols, RFC 5479, April 2009

169. M. Baugher, D. McGrew, M. Naslund, E. Carrara, and K. Norrman. The Secure Real-time Transport Protocol (SRTP), RFC 3711, March 2004

170. J. Franks, P. Hallam-Baker, J. Hostetler, S. Lawrence, P. Leach, A. Luotonen, and L. Stewart. HTTP Authentication: Basic and Digest Access Authentication, RFC 2617, June 1999

171. T. Dierks and E. Rescorla. The Transport Layer Security (TLS) Protocol - Version 1.2, RFC 5246, August 2008

172. J. Fischl, H. Tschofenig, and E. Rescorla. Framework for Establishing a Secure Realtime Transport Protocol (SRTP) Security Context Using Datagram Transport Layer Security (DTLS), RFC 5763, May 2010.

173. D. McGrew and E. Rescorla. Datagram Transport Layer Security (DTLS) Extension to Establish Keys for the Secure Real-time Transport Protocol (SRTP), RFC 5764, May 2010.

174. H. Schulzrinne, H. Tschofenig, C. Holmberg and M. Patel. Public Safety Answering Point (PSAP) Callback, draft-ietf-ecrit-psap-callback (work in progress), March 2012

175. B. Rosen, Requirements for handling abandoned calls and premature disconnects in emergency calls on the Internet, draft-rosen-ecrit-premature-disconnect-rqmts (expired), January 2009.

176. H. Tschofenig, C. Lumbreras. Uniform Resource Name (URN) Namespace for the European Emergency Services, draft-lumbreras-ees-urn-00.txt (work in progress), Oct. 2012.

EENA asbl

info@EENA.org - www.EENA.org

is a non-for-profit association