ATIS-0700015.v005

ATIS Standard on -

ATIS Standard for Implementation of 3GPP Common IMS Emergency Procedures for IMS Origination and ESInet/Legacy Selective Router Termination

As a leading technology and solutions development organization, the Alliance for Telecommunications Industry Solutions (ATIS) brings together the top global ICT companies to advance the industry's most pressing business priorities. ATIS' nearly 200 member companies are currently working to address the All-IP transition, 5G, network functions virtualization, big data analytics, cloud services, device solutions, emergency services, M2M, cyber security, network evolution, quality of service, billing support, operations, and much more. These priorities follow a fast-track development lifecycle — from design and innovation through standards, specifications, requirements, business use cases, software toolkits, open source solutions, and interoperability testing.

ATIS is accredited by the American National Standards Institute (ANSI). The organization is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a founding Partner of the oneM2M global initiative, a member of the International Telecommunication Union (ITU), as well as a member of the Inter-American Telecommunication Commission (CITEL). For more information, visit www.atis.org.

Published by

Alliance for Telecommunications Industry Solutions
1200 G Street, NW, Suite 500
Washington, DC 20005

ATIS-0700015.v005

[Revision of ATIS-0700015.v004]

ATIS Standard on

ATIS Standard for Implementation of 3GPP Common IMS Emergency Procedures for IMS Origination and ESInet/Legacy Selective Router Termination

Alliance for Telecommunications Industry Solutions

Approved June 2021

Abstract

This document identifies and adapts as necessary 3GPP common IMS emergency procedures for applicability in North America to support emergency communications originating from an IMS subscriber (wireline or wireless; fixed, mobile or nomadic) and terminating at an ESInet, or, for appropriate media, legacy emergency services network to support Multimedia Emergency Services (MMES).

It is the intent of this standard to support a full multimedia experience; therefore, simultaneous text, voice, pictures, and video are supported in this standard.

ATIS Standard on –

ATIS Standard for Implementation of 3GPP Common IMS Emergency Procedures for IMS Origination and ESInet/Legacy Selective Router Termination

Foreword

As a leading technology and solutions development organization, the Alliance for Telecommunications Industry Solutions (ATIS) brings together the top global information and communications technology (ICT) companies to advance the industry's most-pressing business priorities. ATIS serves the public through improved understanding between carriers, customers, and manufacturers.

This standard was developed jointly between ESIF, PTSC, and WTSC.

The Emergency Services Interconnection Forum (ESIF) provides a forum to facilitate the identification and resolution of technical and/or operational issues related to the interconnection of wireline, wireless, cable, satellites, Internet and emergency services networks.

The Packet Technologies and Systems Committee (PTSC) develops and recommends standards and technical reports related to services, architectures, and signaling, in addition to related subjects under consideration in other North American and international standards bodies. PTSC coordinates and develops standards and technical reports relevant to telecommunications networks in the U.S., reviews and prepares contributions on such matters for submission to U.S. ITU-T and U.S. ITU-R Study Groups or other standards organizations, and reviews for acceptability or per contra the positions of other countries in related standards development and takes or recommends appropriate actions.

The Wireless Technologies and Systems Committee (WTSC) develops and recommends standards and technical reports related to wireless and/or mobile services and systems, including service descriptions and wireless technologies. WTSC develops and recommends positions on related subjects under consideration in other North American, regional, and international standards bodies.

Suggestions for improvement of this document are welcome. They should be sent to the Alliance for Telecommunications Industry Solutions, WTSC, 1200 G Street NW, Suite 500, Washington, DC 20005.

At the time of initiation or issuance of the letter ballot for this document, the committees responsible for its development had the following leadership:

R. Muscat, ESIF Chair (Bexar Metro 911)
D. Morkunas, ESIF First Vice Chair (Intrado)
J. Torres, ESIF Second Vice Chair (Verizon Wireless)

M. Dolly, PTSC Chair (AT&T)
V. Shaikh, PTSC Vice-Chair (Peraton Labs)

M. Younge, WTSC Chair (T-Mobile)
D. Zelmer, WTSC Vice Chair (AT&T)

F. Khatibi, Technical Editor (Qualcomm)

The **IMSESINET** Subcommittee was responsible for the development of this document.

Table of Contents

Table of Figures

Table of Tables

1 Scope, Purpose, & Application

1.1 Scope

The scope of this standard is to identify and adapt as necessary 3GPP common IP Multimedia Subsystem (IMS) emergency procedures for applicability in North America to support emergency communications originating from an IMS subscriber (fixed, nomadic[1], or mobile) and delivered to a National Emergency Number Association (NENA) i3 Emergency Services IP network (i3 ESInet) and associated NG9-1-1 Core Services (NGCS), or to a legacy Selective Router. ATIS-0700015.v002 specified procedures limited to voice and Global Text Telephony (GTT) [Ref 3] communication. ATIS-0700015.v003 expanded the procedures to incorporate additional multimedia including text, pictures, and video. ATIS-0700015.v004 addressed issues associated with specific transfer models in an i3 ESInet/NGCS. This version, ATIS-0700015.v005, addresses caller authentication in the context of emergency (9-1-1) and callback calls.

While the main focus of this standard is IMS emergency service origination and in particular the associated impacts to an originating device and originating IMS network, the standard also covers related support from the access network and for location acquisition, subscriber home networks in the case of roaming, and considers support for service origination (e.g., callback) from a Public Safety Answering Point (PSAP).

This standard describes the IMS to ESInet interface, as well as the IMS to Selective Router interface. It identifies the types of media that can be delivered to each type of emergency services network.

With respect to 3GPP specifications, the scope of this standard is based upon capabilities defined in Release 16, except where explicitly noted otherwise. With respect to the NENA i3 standard [Ref 100], if there are any discrepancies between this standard and the NENA i3 standard concerning the definition of i3 architecture functional elements, interfaces, or procedures, the NENA i3 standard takes precedence.

1.2 Purpose

The purpose of this standard is to enable deployment in North America of support for Multimedia Emergency Services (MMES) calls[2] in the IP domain from originating networks that conform to 3GPP IMS specifications. The standard is intended to complement the NENA i3 standard [Ref 100] and to define any changes and limitations to the 3GPP IMS solution that are needed for operation in North America.

1.3 Application

The standard applies to support for MMES calls made using IMS in North America. More specifically, it only applies for those MMES services that establish a single SIP session and are able to properly function with only the service logic defined for the P-CSCF and E-CSCF as specified in 3GPP TS 23.167 [Ref 1] and in this standard. Any MMES-based service that requires additional service logic beyond what is defined in this standard, such as may be present in other service platforms like S-CSCFs or AS's as specified in 3GPP TS 23.228 [Ref 34] are for future study.

2 Normative References

The following standards contain provisions which, through reference in this text, constitute provisions of this American National Standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this American National Standard are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below.

[Ref 1] 3GPP TS 23.167, *IP Multimedia Subsystem (IMS) emergency sessions.*[3]

[1] Additional detailed support for nomadic use cases is for further study.

[2] In this standard, the term “calls” is used to mean requests, including voice, texts, etc.

[3] This document is available from the Third Generation Partnership Project (3GPP) at < http://www.3gpp.org/specs/specs.htm >.

[Ref 2] 3GPP TS 24.229, *IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3.* [3]

[Ref 3] 3GPP TS 22.101, *Service aspects; Service principles.* [3]

[Ref 4] 3GPP TS 23.002, *Network architecture.* [3]

[Ref 5] 3GPP TS 23.271, *Technical Specification Group Services and System Aspects; Functional Stage 2 description of Location Services (LCS).*[3]

[Ref 6] IETF RFC 5222, *LoST: A Location-to-Service Translation Protocol*, August 2008.[4]

[Ref 7] J-STD-036-C-2, *Enhanced Wireless 9-1-1 Phase II*, June 2017.[5]

[Ref 8] OMA-TS-MLP-V3_4-20131217-A, *Mobile Location Protocol 3.4, Approved Version 3.4*.[6]

[Ref 9] IETF RFC 6753, *A Location Dereferencing Protocol Using HELD*, October 2012.[4]

[Ref 10] IETF RFC 6155, *Use of Device Identity in HTTP-Enabled Location Delivery (HELD)*, March 2011. [4]

[Ref 11] OMA-TS-ULP-V2_0-20120417-A, *UserPlane Location Protocol*.[6]

[Ref 12] 3GPP TS 36.300, *Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage* 2.[3]

[Ref 13] 3GPP TS 36.331, *Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC*); *Protocol specification*. [3]

[Ref 14] 3GPP TS 23.401, *General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access.* [3]

[Ref 15] 3GPP TS 23.402, *Architecture enhancements for non-3GPP accesses.* [3]

[Ref 16] 3GPP TS 24.301, *Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3.* [3]

[Ref 17] 3GPP2 TS X.S0057-A Version 1.0, *E-UTRAN - eHRPD Connectivity and Interworking: Core Network Aspects.* [3]

[Ref 18] 3GPP TS 23.237, *IP Multimedia Subsystem (IMS) Service Continuity; Stage 2.* [3]

[Ref 19] 3GPP TS 23.216, *Single Radio Voice Call Continuity (SRVCC); Stage 2.* [3]

[Ref 20] 3GPP TS 36.305, *Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Stage 2 functional specification of User Equipment (UE) positioning in E-UTRAN.* [3]

[Ref 21] 3GPP TS 25.401, *UTRAN overall description.* [3]

[Ref 22] 3GPP TS 25.331, *Radio Resource Control (RRC); Protocol specification.* [3]

[Ref 23] 3GPP TS 23.060, *General Packet Radio Service (GPRS); Service description; Stage 2.* [3]

[Ref 24] 3GPP TS 24.008, *Mobile radio interface Layer 3 specification; Core network protocols; Stage 3.* [3]

[Ref 25] 3GPP TS 25.305, *Stage 2 functional specification of User Equipment (UE) positioning in UTRAN.* [3]

[Ref 26] RFC 7852, *Additional Data related to an Emergency Call*.[4]

[Ref 27] 3GPP TS 24.237, *IP Multimedia Subsystem (IMS) Service Continuity; Stage 3.* [3]

[Ref 28] 3GPP TS 29.163, *Interworking between the IP Multimedia (IM) Core Network (CN) subsystem and Circuit Switched (CS) networks*. [3]

[Ref 29] ATIS-1000679, *Interworking between Session Initiation Protocol (SIP) and Bearer Independent Call Control or ISDN User Part.*[5]

[Ref 30] IETF RFC 6442, *Location Conveyance for the Session Initiation Protocol*.[4]

[Ref 31] IETF RFC 4119, *A Presence-based GEOPRIV Location Object Format*.[4]

[Ref 32] IETF RFC 3265, *Session Initiation Protocol (SIP) – Specific Event Notification*.[4]

[Ref 33] IETF RFC 3261, *SIP: Session Initiation Protocol*.[4]

[Ref 34] 3GPP TS 23.228, IP Multimedia Subsystem (IMS); Stage 2.[3]

[4] This document is available from the Internet Engineering Task Force (IETF). < http://www.ietf.org >

[5] This document is available from the Alliance for Telecommunications Industry Solutions (ATIS), 1200 G Street N.W., Suite 500, Washington, DC 20005. < https://www.atis.org/docstore/product.aspx?id=26080 >

[6] This document is available via the Open Mobile Alliance at < http://openmobilealliance.org/ >.

[Ref 35] IETF RFC 5491, *GEOPRIV Presence Information Data Format Location Object (PIDF-LO) Usage Clarification, Considerations, and Recommendations*.[4]

[Ref 36] IETF RFC 5139, *Revised Civic Location Format for Presence Information Data Format Location Object (PIDF-LO)*. [4]

[Ref 37] 3GPP TS 26.114, *Multimedia Telephony; Media handling and interaction*.[3]

[Ref 38] IETF RFC 4975, *The Message Session Relay Protocol (MSRP)*.[4]

[Ref 39] IETF RFC 4976, *Relay Extensions for the Message Session Relay Protocol*.[4]

[Ref 40] ITU-T T.140, *Protocol for multimedia application text conversation*.[7]

[Ref 41] IETF RFC 5031, *A Uniform Resource Name (URN) for Emergency and Other Well-known Services*.[4]

[Ref 42] IETF RFC 3455, *Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)*.[4]

[Ref 43] IETF RFC 4244, *An Extension to the Session Initiation Protocol (SIP) for Request History Information*.[4]

[Ref 44] IETF RFC 3325, *Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks*.[4]

[Ref 45] ATIS-1000074-E, *Errata on ATIS Standard on Signature-based Handling of Asserted information using toKENs (SHAKEN)*.[5]

[Ref 46] ATIS-1000082, *Technical Report on SHAKEN API for a Centralized Signing and Signature Validation Server.*[5]

[Ref 47] IETF RFC 7230, *Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing.*[4]

[Ref 48] IETF RFC 8225, *PASSporT: Personal Assertion Token.*[4]

[Ref 49] IETF RFC 8443, *Personal Assertion Token (PASSporT) Extension for Resource Priority Authorization.*[4]

[Ref 50] IETF RFC 8224, *Authenticated Identity Management in the Session Initiation Protocol (SIP).*[4]

[Ref 51] IETF RFC 9027, *Assertion Values for Resource Priority Header and SIP Priority Header Claims in Support of Emergency Services Networks*.[4]

[Ref 52] IETF RFC 7090, *Public Safety Answering Point (PSAP) Callback.*[4]

[Ref 53] IETF RFC 7135, *Registering a SIP Resource Priority Header Field Namespace for Local Emergency Communications*.[4]

[Ref 54] IETF RFC 4122, *A Universally Unique IDentifier (UUID) URN Namespace*.[4]

3 Informative References

The following standards contain provisions which, through reference in this text, constitute provisions of this ATIS Standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this ATIS Standard are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below.

[Ref 100] NENA-STA-010.2, *NENA Detailed Functional and Interface Standards for the NENA i3 Solution*, September 10, 2016.[8]

[Ref 101] NENA-ADM-000.23-2020, *NENA Master Glossary of 9-1-1 Terminology.*[8]

[Ref 102] NENA-STA-015.10-2018, *NENA Standard Data Formats for E9-1-1 Data Exchange & GIS Mapping.*[8]

[7] This document is available from the ITU-T http://www.itu.int/rec/T-REC-T.140/en

[8] This document is available from the National Emergency Number Association.
< http://www.nena.org/?page=Standards >

4 Definitions, Acronyms, & Abbreviations

4.1 Definitions

Term	Definition
Associated Location	An Associated Location is a location (civic, geodetic, or polygon) within the designated PSAP jurisdiction that may be used in wireless call scenarios to route the call toward the designated PSAP.
Core Network Entity	The Core Network Entity is a functional entity in the packet core network that interfaces to a Location Server. For example, see Figure C.2, Steps 2 and 6, where the *core network entity* for LTE access is the Mobility Management Entity (MME).
Emergency Services Routing Digits (ESRD)	J-STD-036-C-2 [Ref 7] defines an ESRD as, "A digit string that uniquely identifies a base station, cell site, or sector that may be used to route emergency calls through the network." In the context of this standard, a Reference Identifier will contain an ESRD if an emergency session request received by an E-CSCF/LRF (Emergency Call Session Control Function/Location Retrieval Function) contains an MDN/MSISDN (Mobile Directory Number/ Mobile Subscriber ISDN Number) and cell site/sector information, and the call is to be routed to a legacy Selective Router that supports receipt of both ESRD and callback number over the incoming trunk group from the IMS Origination Network.
Emergency Services Routing Key (ESRK)	J-STD-036-C-2 [Ref 7] defines an ESRK as, "A digit string that uniquely identifies an ongoing Emergency Services Call and it is used to correlate the Emergency Services Call with the associated data messages. It may also identify an Emergency Services Zone and it may be used to route the call through the network." In the context of this standard, a Reference Identifier will contain an ESRK if an emergency session request received by an E-CSCF/LRF contains an MDN/MSISDN and cell site/sector information, and the call is to be routed to a legacy Selective Router that supports receipt of an ESRK over the incoming trunk group from the IMS Origination Network.
Multimedia Emergency Services (MMES)	MMES are next generation emergency services utilizing real-time session-based text and other multimedia, including voice, that are based on trusted applications in support of non-voice communications between citizens and Public Safety. MMES provide secure transport of messaging and media content, and location information of the reporting device to Public Safety, in addition to providing two-way voice emergency communications between citizens and Public Safety. It is assumed that the UE has a SIP client capable of initiating an MMES session and the Common IMS network will forward that request to an emergency network capable of handling the session.
Nomadic	In the context of location information to support IP-based emergency services, a user is said to be nomadic if the user has the ability to change location only in between sessions but not during a session. The user equipment is constrained within an access network such that its location can be represented as a definitive civic address or geo coordinates for that network attachment. The user may move from one network attachment to another but cannot maintain a session during that move. If the user is able to move outside the definitive civic address or geo coordinates without losing network attachment, then the user is considered to be mobile, not nomadic.
Public Safety Answering Point (PSAP)	The PSAP is an entity operating under common management which receives 9-1-1 calls from a defined geographic area and processes those calls according to a specific operational policy.
Reference Identifier	The term "Reference Identifier" is used in this standard to associate the call with location information of the caller. For routing to a legacy emergency services network, a Reference Identifier may be an Emergency Services Routing Key (ESRK) or Emergency Services Routing Digit (ESRD) as defined in J-STD-036-C-2 [Ref 7]. It may be the Telephone Number that is used by the legacy emergency services network to query for location information. In a legacy emergency services network, the Reference Identifier may also be used by the emergency services network to route the call to the PSAP. For calls routed to a NENA i3 ESInet, the Reference Identifier may be a dereferencing URI that is used by NENA i3 functional elements and NENA i3 PSAPs to obtain location.

Term	Definition
Validate	The term “Validate” is used in this standard to describe the method used to check that a civic address precisely matches an entry in an appropriate authoritative source. For legacy networks, the authoritative source is a Master Street Address Guide (MSAG). For Next Generation 9-1-1 (NG9-1-1), validation is based on Geographic Information System (GIS) data using the Location Validation Function (LVF).

4.2 Acronyms & Abbreviations

1x RTT	single carrier Radio Transmission Technology for cdma2000
ALI	Automatic Location Identification
ATIS	Alliance for Telecommunications Industry Solutions
BCF	Border Control Function
BGCF	Breakout Gateway Control Function.
CAMA	Centralized Automatic Message Accounting
cpc	Calling Party's Category
CS	Circuit Switched
CSCF	Call Session Control Function
CVT	Call Validation Treatment
EATF	Emergency Access Transfer Function
ECRF	Emergency Call Routing Function
ECS	Emergency Call Server
E-CSCF	Emergency Call Session Control Function
EDGE	Enhanced Data rates for GSM Evolution
eHRPD	evolved High Rate Packet Data
FQDN	Fully Qualified Domain Name
ELIA	Emergency Location Immediate Answer
ELIR	Emergency Location Immediate Request
ELR	Emergency Location Report
EPC	Evolved Packet Core
ESInet	Emergency Services IP network
E-SLP	Emergency SLP
E-SMLC	Enhanced Serving Mobile Location Center
ESRD	Emergency Services Routing Digits
ESRK	Emergency Services Routing Key
ESRP	Emergency Service Routing Proxy
GDP	Generic Digits Parameter
GERAN	GSM EDGE Radio Access Network
GIS	Geographic Information System
GMLC	Gateway Mobile Location Center
GPRS	General Packet Radio Service
GSM	Global System for Mobile communications
GRUU	Globally Routable User Agent URI
GTT	Global Text Telephony
HELD	HTTP-Enabled Location Delivery
HRPD	High Rate Packet Data
H-SLP	Home SLP

HSPA	High Speed Packet Access
HSS	Home Subscriber Server
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP Secure
IBCF	Interconnection Border Control Function
I-CSCF	Interrogating CSCF
IETF	Internet Engineering Task Force
IMEI	International Mobile Equipment Identity
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IP-CAN	IP Connectivity Access Network
ISDN	Integrated Services Digital Network
IWS	Interworking Solution function
LbyR	Location-by-Reference
LbyV	Location-by-Value
LCS	LoCation Services
LPP	LTE Positioning Protocol
LRF	Location Retrieval Function
LS	Location Server
LTE	Long Term Evolution
MDN	Mobile Directory Number
MEID	Mobile Equipment IDentifier
MF	Multi-Frequency
MGCF	Media Gateway Control Function
MIN	Mobile Identification Number
MLP	Mobile Location Protocol
MME	Mobility Management Entity
MMES	Multimedia Emergency Services
MPC	Mobile Position Center
MSAG	Master Street Address Guide
MSC	Mobile Switching Center
MSISDN	Mobile Subscriber ISDN Number
NENA	National Emergency Number Association
NG9-1-1	Next Generation 9-1-1
NGCS	NG9-1-1 Core Services
NI-LR	Network Induced Location Request
NPA	Numbering Plan Area
oli	Originating Line Information
OMA	Open Mobile Alliance
PAI	P-Asserted Identity
PASSporT	Personal Assertion Token
P-CSCF	Proxy CSCF
PDN	Packet Data Network
PDP	Packet Data Protocol

PSAP	Public Safety Answering Point
PSTN	Public Switched Telephone Network
PTSC	Packet Technologies and Systems Committee
QoS	Quality of Service
RAN	Radio Access Network
RDF	Routing Determination Function
RNC	Radio Network Controller
RPH	Resource-Priority Header
RRC	Radio Resource Control
RRLP	Radio Resource LCS Protocol
RTT	Round Trip Time
SAI	Service Area Identifier
SBC	Session Border Controller
S-CSCF	Serving CSCF
SGSN	Serving GPRS Support Node
SHAKEN	Signature-based Handling of Asserted information using toKENs
SKS	Secure Key Store
SLP	SUPL Location Platform
SR	Selective Router
STI	Secure Telephone Identity
STI-AS	Secure Telephone Identity Authentication Service
STI-CR	Secure Telephone Identity Certificate Repository
STIR	Secure Telephone Identity Revisited
STI-VS	Secure Telephone Identity Verification Service
SUPL	Secure User Plane Location
TCP	Transmission Control Protocol
TN	Telephone Number
TR	Technical Report
UDP	User Datagram Protocol
UE	User Equipment
UMTS	Universal Mobile Telecommunications System
USIM	Universal Subscriber Identity Module
UTRAN	Universal Terrestrial Radio Access Network

5 Introduction

The emergency services landscape within North America requires a greater level of detail than what has been specified in 3GPP. This document provides additional details with respect to emergency services for North America, specific to interconnection to both legacy emergency service networks and next generation emergency services networks. This standard uses 3GPP standards as its base and consideration must be given to how the specific aspects of the 3GPP standards apply within the context of the North American architecture.

North American IMS-based origination networks originate emergency calls (which include steps taken by the originating device and network elements) and route such calls to a NENA i3/NG9-1-1 ESInet (initial ingress ESInet) or legacy Selective Router. As part of call handling within the IMS origination network, the location (or an estimated location) of the originating device is determined and used to route the call to an appropriate ESInet entry point or to a legacy Selective Router. This location, or an updated and possibly more accurate version (via re-bid), can be made available to PSAPs for dispatch.

This standard identifies the types of media that can be delivered to each type of emergency services network, i.e., legacy emergency services network and a NENA i3 ESInet. For example, voice, GTT, and session-mode text can be delivered to a legacy emergency services network via interworking. All types of media can be delivered to a NENA i3 ESInet.

This standard also describes the impacts on IMS originating networks of applying the Signature-based Handling of Asserted information using toKENs (SHAKEN) framework, as specified in ATIS-1000074-E **Error! Reference source not found.**, to 9-1-1 calls and callback calls. The SHAKEN framework provides a general architecture to support service provider caller identity authentication and verification services based on the protocols defined in the IETF Secure Telephone Identity Revisited (STIR) Working Group. In addition to caller identity authentication/verification, 9-1-1 calls and callback calls may be subject to Resource-Priority Header (RPH) signing, and callback calls may be subject to SIP Priority header signing. Compromise of the SIP RPH field could lead to misuse of network resources (e.g., during congestion scenarios). The SIP Priority header field allows special network handling and routing of emergency callbacks. It is important to protect and validate the authoritative use of these fields.

This document is intended to be a standalone standard that by itself describes IP emergency call support for IMS networks and includes North American-specific requirements – e.g., on Reference Identifier assignment and location support, that in 3GPP documents are more generic.

The intent of this document is to concentrate on common IMS-based origination networks supporting all classes of service; IMS aspects are mostly access-independent and not limited to mobile.

Clause 6 provides basic assumptions as well as assumptions specific to support for caller identity authentication and verification, and RPH and SIP Priority header signing/verification. Clause 6 also defines requirements via reference to 3GPP specifications, and includes any differences (e.g., extensions or restrictions) to these specifications.

Clause 7 provides an architectural description that is based on the IMS architecture defined for 3GPP and the ESInet architecture for NENA i3 [Ref 100]. Clause 7 also describes some extensions to the 3GPP IMS architecture applicable to operation in North America, and provides a brief definition of each of the main architectural entities within the IMS originating network and the emergency services networks.

Clause 8 provides a description of the procedures and signaling applicable to location retrieval and emergency call origination to a NENA i3 ESInet and legacy emergency services network.

Clause 9 provides a description of any differences to existing standards including use of particular options regarding treatment of different access types for support of IMS Emergency Calls in North America.

Annex A provides a normative SIP INVITE profile for the ici reference point between the Interconnection Border Control Function (IBCF) in the IMS originating network and the Border Control Function (BCF) in the ESInet.

Annex B provides a normative description of using the Mobile Location Protocol (MLP) between the Location Retrieval Function (LRF) and Location Server (LS) for L0.

Annex C provides an informative description of location acquisition and conveyance based on the 3GPP Control Plane and OMA User Plane location solutions for Long Term Evolution (LTE) and High Speed Packet Access (HSPA).

Annex D provides an informative description of emergency call routing by an IMS originating network.

Annex E is an informative Annex that describes message examples for various use cases.

Annex F is an informative Annex that describes some of the access network types for which the procedures and requirements in this document are applicable, with specific reference to IMS interaction, handover, and support of location. For each access type, capabilities and requirements are summarized with references to the applicable standards in which they are fully defined.

Annex G is an informative Annex that describes a set of use cases for an IMS emergency call origination, to legacy PSAPs as well as IP-capable PSAPs, routing on geographic location or cell site/sector, and use of location-by-value or location-by-reference.

Annex H is an informative Annex that describes the UE originating a call with location-by-reference.

6 Assumptions & Requirements

This clause describes assumptions and requirements applicable to this standard.

6.1 Basic Assumptions

1. This standard supports fixed, nomadic, and mobile callers.
2. This standard is aligned with 3GPP Release 16; with North American extensions/restrictions.
3. Emergency calls egress to either a legacy emergency services network or an IP-based emergency services network (i.e., NENA i3/NG9-1-1 ESInet [Ref 100]).
4. For MMES sessions, the Common IMS network will determine the appropriate emergency services network (e.g., a NENA i3 ESInet).
5. MMES sessions beyond voice and GTT cannot be routed to legacy emergency services networks.
6. Each User Equipment (UE) contains an IMS client.
7. A UE may or may not be location aware.
8. Methods of location determination are outside the scope of this standard.
9. If there is a civic address associated with the UE, it is validated; the validation process is out of the scope of this standard.
10. An Associated Location is used in some wireless routing scenarios where the cell address or cell centroid cannot be used to route a call to the ESInet or the Selective Router.
11. An originating network and UE may support some or all media types.
12. It may be possible to negotiate the user's indicated desired language(s), per media stream and/or session, in order of preference.
13. Voice and GTT sessions are expected to be maintained when a UE with an active IMS MMES moves out of IMS emergency coverage.
14. This standard only addresses emergency service use of IMS services. It does not address use of legacy services (e.g., SMS to 9-1-1) in an emergency or the interworking of legacy services with IMS.

6.2 Assumptions Associated with Caller Identity, RPH and SIP Priority Header Signing/Verification

1. A Resource-Priority Header (RPH) in the ‘esnet’ namespace may or may not be associated with an emergency origination by the originating IMS network, based on local policy.
2. Caller identity assertion/authentication and/or RPH signing will be performed by the originating network after it has been determined that the emergency call is to be routed to an i3 ESInet/ NGCS.
3. Signing of caller identity is separate from SIP RPH/Priority header signing. Separate SIP Identity headers are used for SIP RPH/Priority header signing and caller identity signing.
4. A Service Provider can use the same certificates for signing SIP RPH/Priority header as they use for telephone number (TN) signing, but is not required to do so.
5. The i3 ESInet/NGCS will be responsible for performing verification of Personal Assertion Token (PASSporT) information received with an emergency call.
6. The originating network provider will be notified by the i3 ESInet/NGCS if verification fails, as described in Clause 5.3.2 of ATIS-1000074-E **Error! Reference source not found.**.
7. The i3 ESInet/NGCS will be responsible for performing caller identity attestation/authentication and RPH and SIP Priority header signing on callback calls.
8. Callback calls will use normal routing (i.e., via the emergency caller’s home network) to the network that is serving the emergency caller.
9. Callback calls received by the emergency caller’s home network will be marked as “psap-callback” and will contain an RPH with a value of “esnet.0”.
10. Verification of signed caller identity/RPH/SIP Priority header information will be performed by the terminating home network for the callback call.

11. Analytics, via the Call Validation Treatment (CVT) function defined in ATIS-1000074-E **Error! Reference source not found.**, may be applied to a callback call based on local policy and agreements between the home network provider and the analytics/CVT provider.
12. Privacy of caller identity information associated with callback calls will be supported/preserved.
13. If verification of the signed caller identity or SIP RPH/Priority header associated with a callback call is successful, verification status information associated with the callback call is sent to the emergency caller's User Equipment (UE).
14. If validation of the signed caller identity or SIP RPH/Priority header associated with a callback call fails, home network provider local policy will determine terminating call processing, such as whether the call should be delivered with caller identity and/or SIP RPH and Priority header information intact. Note that if the call proceeds, verification status information will be included in the associated SIP signaling, as described above.
15. SIP RPH signing does not change or modify 9-1-1/callback call processing, signaling and routing procedures; it simply provides a security tool for transit and receiving providers to determine if the SIP RPH is trusted.

6.3 Requirements

The Architectural Principles defined in Clause 4.1 of 3GPP TS 23.167 [Ref 1] and 3GPP TS 24.229 [Ref 2] apply to this standard with the differences and clarifications noted below. Parts of that section are copied as required to illustrate the differences and clarifications.

3GPP TS 23.167 [Ref 1], Clause 4.1: "If required, the E-CSCF shall be able to forward the location information to the LRF for validation of geographical location information in the case that the geographical location information is included by the UE over any access network type."

Architecture-Principles-010 – The LRF shall not validate geographical location information during an emergency session.

NOTE: Any civic location must be validated against an emergency services validation database prior to the origination of an emergency session. Geo-coordinate locations cannot be validated. Geo-coordinate locations can only be verified to be within expected boundaries.

3GPP TS 23.167 [Ref 1], Clause 4.1: "The E-CSCF is the IMS network entity, which is responsible to route the request to an emergency center/PSAP or BGCF based on location information and additionally other information such as type of emergency service in the request."

Architecture-Principles-020 – The E-CSCF shall route the emergency session (e.g., to the MGCF via BGCF for the legacy emergency services network or IBCF for the ESInet) based upon routing information received from the LRF.

3GPP TS 23.167 [Ref 1], Clause 6.2.1: "Reject/allow anonymous emergency requests."

P-CSCF-010 Based on the operator's policy, the P-CSCF shall allow anonymous emergency requests.

The Emergency-CSCF Clause 6.2.2, of 3GPP TS 23.167 [Ref 1] applies to this standard, with the clarifications noted below.

3GPP TS 23.167 [Ref 1], Clause 6.2.2: "If the UE does not have credentials, a non-dialable callback number shall be derived where required by local regulation (e.g. see Annex C of J-STD-036 [23])."

E-CSCF-010 For an emergency session originated from a mobile device, the E-CSCF shall always follow Annex C of J-STD-036-C-2 [Ref 7] to derive a non-dialable callback number for a UE that does not have credentials. The E-CSCF shall populate the P-Asserted-Identity (PAI) with the non-dialable number before it sends the SIP INVITE to the LRF.

3GPP TS 23.167 [Ref 1], Clause 6.2.2: “If location information is not included in the emergency request or additional location information is required, the E-CSCF may request the LRF to retrieve location information as described in 7.6, *Retrieving Location Information for Emergency Session*.”

E-CSCF-020 The E-CSCF shall always interact with the LRF to determine routing and allow the LRF to acquire location if appropriate.

E-CSCF-030 The E-CSCF shall pass the session request, including all information received from the P-CSCF, to the LRF.

NOTE 1: This includes all headers and the SIP body that may include PIDF-LO and SDP.

3GPP TS 23.167 [Ref 1], Clause 6.2.2: “Determines or queries the LRF for the proper routing information/PSAP destination.”

NOTE 2: See E-CSCF-020**.**

3GPP TS 23.167 [Ref 1], Clause 6.2.2: “Subject to local regulation, the E-CSCF may send the contents of the P-asserted ID or UE identification to the LRF.”

NOTE 3: See E-CSCF-030.

Additional requirements for the E-CSCF:

E-CSCF-040 The E-CSCF shall indicate to the LRF that the call has been terminated, if the LRF requests such notification.

NOTE: This may be used by the LRF to manage resources such as Reference Identifiers.

The Procedures at the E-CSCF Clause 5.11.1 of 3GPP TS 24.229 [Ref 2] applies to this standard with the clarifications noted below.

3GPP TS 24.229 [Ref 2], Clause 5.11.1: “When the E-CSCF receives an emergency request for a dialog requesting privacy or a standalone emergency transaction requesting privacy or any request or response related to a UE-originated emergency dialog requesting privacy, and if operator policy (e.g., determined by national regulatory requirements applicable to emergency services) allows requests for suppression of public user identifiers and location information per 3GPP TS 22.101 [Ref 3], the E-CSCF:

“- Shall provide the privacy service role according to RFC 3323 [33] and RFC 3325 [34];

“NOTE 3: The procedure above is in addition to any procedure for the application of privacy at the edge of the trust domain specified by RFC 3325 [34] and Clause 4.4.

“- Shall remove any location object from the message’s body with Content-Type header field containing the content type application/pidf+xml. If only one message body remains in the message’s body then the E-CSCF sets the Content-Type header field to the content type specified for the body; and

“- Shall remove the Geolocation header field; prior to forwarding any such request to a PSAP.”

“NOTE 4: If the routing functions are supported by an LRF, this information is not removed before the request is sent to the LRF.”

E-CSCF-050 The above “dialog requesting privacy or a standalone emergency transaction requesting privacy” shall not be supported in North America.

NOTE: In North America, the ESInet relies on the originating network supplying a Geolocation header. This version of the standard does not address methods to protect the UE privacy (e.g., for government officials).

E-CSCF-060 An E-CSCF shall be capable of processing a SIP 300 Multiple Choices message in which location-by-value or location-by-reference is returned, and generating an outgoing SIP INVITE message following the procedures defined in Clause 5.11.3 of 3GPP TS 24.229 [Ref 2].

NOTE: 3GPP includes procedures in 3GPP TS 24.229 [Ref 2] that support the use of RFC 3261-based [Ref 33] mechanisms for returning location-by-reference and location-by-value to an E-CSCF in a SIP 300 Multiple Choices response from an LRF. 3GPP TS 24.229 [Ref 2] specifies that support of such procedures is based on operator policy. These procedures will be supported by E-CSCFs operating in North America, as defined in this standard.

E-CSCF-070 An E-CSCF shall be capable of processing a SIP 300 Multiple Choices message in which Additional Call Data "by-reference" or "by-value" (see IETF RFC 7852 [Ref 26]) is returned, and generating an outgoing SIP INVITE message following the procedures defined in RFC 3261 [Ref 33], Clause 19.1.5, with the clarifications described in Clause 8.5.1.

NOTE: Non-location information, such as service provider contact information and class of service information, is provided to legacy PSAPs today via the Automatic Location Identification (ALI) system. PSAPs connected to a NENA i3 ESInet will continue to require that this non-location "Additional Call Data" be provided for incoming emergency calls. Additional Call Data can be provided either "by-reference" or "by-value," as determined by the sender of the information.

E-CSCF-080 If, based on the format of the URI in the Contact header of the SIP 300 Multiple Choices response, the E-CSCF determines that the emergency call is to be routed to a PSAP served by an i3 ESInet, the E-CSCF shall place the URI received in the Contact header field in the topmost entry in the Route header field, following the procedures defined in Clause 5.11.3 of 3GPP TS 24.229 [Ref 2], and shall ensure that the Replaces option tag is not included in the Supported header of the outgoing SIP INVITE message. (See Clause 8.5.1 for further details.)

NOTE: If the emergency call is destined for a PSAP that is served by a NENA i3 ESInet, and the initial SIP INVITE message received by the E-CSCF includes a Replaces option tag in the Supported header, the E-CSCF will remove the Replaces option tag from the Supported header before forwarding the SIP INVITE message to the egress IBCF.

The description of the Location Retrieval Function, as specified in Clause 6.2.3 of 3GPP TS 23.167 [Ref 1], applies to this standard with the clarifications noted below.

LRF-010 If a location value was not received by the LRF in the request from the E-CSCF, the LRF shall initiate the process to acquire the location.

LRF-020 When the LRF acquires location, it may cache it in anticipation of a query from a requesting entity (e.g., the PSAP).

LRF-030 If the LRF receives or acquires a location that may change (either because the user equipment is a mobile device or because location accuracy can be improved), it shall allocate a Reference Identifier and return it to the E-CSCF.

LRF-040 If the LRF acquires a location that will not change (e.g., fixed line), and it is routing to an ESInet, then the LRF shall return the location object (location-by-value) rather than the Reference Identifier.

LRF-050 For calls destined to a legacy emergency services network, the Reference Identifier shall be a 10 digit number within NPA ranges supported by the destination PSAP.

NOTE: Current Centralized Automatic Message Accounting (CAMA) PSAPs support only four (4) Numbering Plan Areas (NPAs) and so the Reference Identifier must be drawn from a pool within one of these NPAs.

LRF-060 For calls destined to an ESInet, the Reference Identifier must be globally unique.

NOTE: There are no NPA restrictions and, in fact, the Reference Identifier need not be a Telephone Number (TN).

LRF-070 The LRF shall support the capability to return the current information that it has to a location query (e.g., in response to an initial query or depending on query parameters).

LRF-080 The LRF shall support the capability to return the results of a location acquisition process in a response to a location query (e.g., depending on query parameters).

LRF-090 The LRF shall request that the E-CSCF provide notification when the call has been terminated if the LRF allocates a Reference Identifier to the emergency call. If the LRF does not allocate a Reference Identifier to the emergency call, it may request that the E-CSCF provide notification when the call has been terminated.

NOTE: Notification of call termination will be used by the LRF to manage resources such as Reference Identifiers (if applicable). If notification of call termination is not received by the LRF in response to its request, operator policy will determine the mechanism used to trigger release of the Reference Identifier allocated to the emergency call.

LRF-100 The LRF shall be able to provide Additional Call Data as specified in RFC 7852 [Ref 26] to the E-CSCF if required by operator policy.

LRF-110 For mobile emergency calls using control plane location services, the LRF shall support location continuity (e.g., after a handover to a new core network entity, the LRF will invoke the LS associated with the new core network entity).

LRF-120 If a location value is not received by the LRF in the request from the E-CSCF, and the LRF is unable to acquire a location to associate with the call, the LRF shall return a default Route URI value (configured in the LRF) in the Contact header of the SIP 300 Multiple Choices message returned to the E-CSCF.

LRF-130 If, after sending a routing request to a Routing Determination Function (RDF), the LRF does not receive a response within an operator settable timeout, or the LRF receives an error response from the RDF, the LRF shall return a default Route URI value (configured in the LRF) in the Contact header of the SIP 300 Multiple Choices message returned to the E-CSCF.

LRF-140 If the LRF receives the address of the LS in a report [i.e., Emergency Location Report (ELR)], the LRF shall direct location queries to that address until such time as the LRF receives:

- A subsequent report that includes a new LS address.
- A subsequent report that includes a target serving core network identity and no LS address.
- A location response that contains a target serving core network identity.

LRF-150 If the LRF receives a report (i.e., ELR) or a location response from an LS that contains a target serving core network identity and no LS address, the LRF shall determine the address of the LS to which subsequent location requests will be directed.

NOTE: The details of the mechanism used to determine the address of the LS in this scenario are left to implementation.

LRF-160 If the LRF receives a report (i.e., ELR) or location response from an LS that contains the identity of the serving core network identity, the LRF shall include the most recently received serving core network identity in location requests that it generates.

LRF-170 If the LRF receives a SIP INVITE from the E-CSCF with a PAI having a non-dialable number, the LRF shall use the Instance ID (that contains the IMEI) within the Contact header field as a key to acquire the location from the LS when using MLP.

LRF-180 If the LRF receives a SIP INVITE from the E-CSCF with a PAI having a non-dialable number, the LRF shall use the non-dialable callback number and the cell identifier as keys to acquire the location from the LS when using E2.

LS-010 When the LS receives a request from the LRF for the location of a UE, the LS shall acquire the location of the requested UE and provide the response to the LRF.

LS-020 If the network supports mobile emergency calls and control plane location services, and the LS receives the identity of the serving core network entity in a report or a location response, the LS shall report the identity of the serving node to the LRF.

LS-030 If the network supports mobile emergency calls and control plane location services, then the LS shall report its address to the LRF upon receiving a report that emergency bearer services have been originated by a UE.

LS-040 If the network supports mobile emergency calls and control plane location services, a change in serving core network entity has occurred, and the target LS initiates a report to the LRF, the target LS shall report its address to the LRF.

LS-050 If the network supports mobile emergency calls and control plane location services, a change in serving core network entity has occurred such that the new core network entity is not associated with the source LS, and the source LS initiates a report to the LRF, the source LS shall not include an LS address in its report to the LRF.

RDF-010 The RDF shall determine the appropriate emergency services network and return routing information to the E-CSCF via the LRF.

RDF-020 If the RDF is unable to determine the appropriate emergency services network, it shall return default routing information to the E-CSCF via the LRF.

Clause 5.10.2.2 of 3GPP TS 24.229 [Ref 2], which describes exit point IBCF behavior associated with initial requests, applies to this standard with the clarification noted below:

IBCF-010 An egress IBCF shall not include Replaces in the Supported header of a SIP INVITE message associated with an emergency call that is destined for a NENA I3 ESInet.

6.4 Requirements Associated with Caller Identity, RPH and SIP Priority Header Signing/Verification

SHAKEN-P-CSCF-010 If the P-CSCF detects that the Request-URI of the initial request for a dialog matches one of the emergency service identifiers in the associated lists, the P-CSCF shall add a Resource-Priority header field set to "esnet.1" as defined in RFC 7135 [Ref 53], if the network uses the Resource-Priority header field to control the priority of emergency calls.

SHAKEN-P-CSCF-020 If a P-CSCF is operating in a network that supports calling number verification using signature verification and attestation information as specified in subclause 3.1 of 3GPP TS 24.229 and, based on local policy, the P-CSCF performs attestation of a caller identity in an incoming emergency call request, the P-CSCF shall convey the results of the attestation process by populating an attestation level of "A", "B", or "C" (as specified in ATIS-1000074-E) in an Attestation-Info header field within the outgoing SIP INVITE message.

SHAKEN-P-CSCF-030 If a P-CSCF has performed attestation of a caller identity in an incoming emergency call request, then based on local policy, the P-CSCF shall add an Origination-Id header, in the form of a string, to the outgoing SIP INVITE message to identify the node that performed the attestation. The origination identifier should be a unique string corresponding to a Universally Unique Identifier (UUID) [Ref 54]. The value populated in the Origination-Id header field shall be based on local configuration and regulation.

SHAKEN-P-CSCF-040 If a P-CSCF provides attestation information associated with the caller identity associated with an emergency call request then, based on local policy, the P-CSCF shall insert a "verstat" parameter in the P-Asserted-Identity header or From header.

SHAKEN-IBCF-010 An exit IBCF in an IMS originating network that supports caller identity authentication and RPH signing associated with emergency call requests shall send an HTTP POST message that contains one signingRequest associated with the caller identity and one signingRequest associated with the RPH over the Ms reference point to the STI-AS.

SHAKEN-IBCF-020 Based on local policy, an exit IBCF in an IMS originating network that supports caller identity authentication and RPH signing associated with emergency call requests shall populate the parameters in the signing requests directly based on header fields received in the incoming SIP INVITE message (e.g., the Attestation-Info, Origination-Id), if available. If the header fields are not available, the IBCF shall derive the information to populate the claims in the signing requests based on other information in the SIP INVITE message or based on provisioning.

SHAKEN-IBCF-030 An exit IBCF in an originating IMS network that supports caller identity authentication and RPH signing associated with emergency call requests shall, upon receiving an emergency call request with a non-dialable callback number formatted per Annex C of J-STD-036-C-2 in the P-Asserted-Identity header, populate the non-dialable callback number in the "orig" parameter of the signingRequest, a value of "A" in the "attest" parameter of the signingRequest, and shall populate the remaining parameters as it would for a 9-1-1 call with a dialable callback number.

SHAKEN-IBCF-040 An exit IBCF in an originating IMS network that supports caller identity authentication and RPH signing associated with emergency call requests shall be capable of receiving and processing an HTTP 200 OK

message that contains two signing responses, each including an identityHeader parameter. The exit IBCF shall use the identityHeader parameters to populate Identity header fields (one associated with the signed caller identity and one associated with the signed RPH) in the outgoing SIP INVITE message.

SHAKEN-IBCF-050 An exit IBCF in an IMS originating network that supports caller identity authentication and RPH signing associated with emergency call requests shall remove any "verstat" information that is present in the P-Asserted-Identity or From header fields before forwarding the SIP INVITE message to the interconnecting i3 ESInet/NGCS.

SHAKEN-IBCF-060 An exit IBCF in an IMS originating network that supports caller identity authentication and RPH signing associated with emergency call requests may, based on local policy, make a determination as to what information (other than "verstat", which as indicated in SHAKEN-IBCF-050, must not be forwarded) related to caller identity authentication and RPH signing should be forwarded to the interconnected Emergency Services Network based on the capabilities of that network.

SHAKEN-IBCF-070 An entry IBCF in an IMS home network that supports caller identity, RPH, and SIP Priority header verification associated with emergency callbacks shall remove the "verstat" parameter from an incoming SIP INVITE message associated with an emergency callback that contains a "verstat" populated as a tel uri parameter in the P-Asserted-Identity header field or From header field.

SHAKEN-IBCF-080 An entry IBCF in an emergency caller's home network that has implemented the Ms reference point between the entry IBCF and the Verification Service to support verification of caller identity, RPH, and the SIP Priority header for emergency callbacks, shall send an HTTP verificationRequest to the STI-VS that contains an identityHeader parameter populated based on the Identity header associated with the caller identity, and an identityHeaders parameter containing the Identity header information associated with the RPH/Priority header received in the incoming SIP INVITE message associated with the emergency callback.

SHAKEN-IBCF-090 An entry IBCF in an emergency caller's home network that has implemented the Ms reference point between the entry IBCF and the Verification Service to support verification of caller identity, RPH, and the SIP Priority header for emergency callbacks, shall be capable of receiving and processing an HTTP OK message containing a verificationResponse from the STI-VS.

SHAKEN-IBCF-100 An entry IBCF in an emergency caller's home network that has implemented the Ms reference point between the entry IBCF and the STI-VS to support verification of caller identity, RPH, and the SIP Priority header for emergency callbacks shall use the verstatValue parameter received in the verificationResponse within an HTTP 200 OK message to populate "verstat" information as a tel uri parameter in the P-Asserted-Identity header field (or the From header field, if no P-Asserted-Identity header field is present) of the forwarded SIP INVITE message. The entry IBCF shall use the verstatPriority parameter in the verificationResponse to populate the Priority-Verstat header field in the forwarded SIP INVITE message.

SHAKEN-S-CSCF-010 If an emergency caller's home network supports caller identity, RPH, and SIP Priority header verification associated with emergency callbacks by having an S-CSCF interact with the STI-VS, the S-CSCF shall forward the incoming SIP INVITE message to the STI-VS prior to applying other call processing to the call. Upon receipt of the SIP INVITE message back from the STI-VS with verification status information populated (i.e., in the form of a "verstat" tel uri parameter in the P-Asserted-Identity header field [or the From header field, if no P-Asserted-Identity header field is present], and in a Priority-Verstat header field), the S-CSCF shall continue processing the emergency callback as specified below.

SHAKEN-S-CSCF-020 The S-CSCF shall follow the procedures specified in Clause 5.3.1 of ATIS-1000074-E regarding the sending of "verstat" information to an emergency caller's UE in the From or P-Asserted-Identity header field of an INVITE request associated with an emergency callback.

SHAKEN-S-CSCF-030 If the Priority-Verstat header field received from the STI-VS contains a value of "ECB-RPH-Validation-Passed", the S-CSCF shall pass the Priority-Verstat header field forward in the INVITE request associated with the emergency callback. If the Priority-Verstat field received from the STI-VS contains a value other than "ECB-RPH-Validation-Passed", the S-CSCF shall use local policy to determine whether to forward the Priority-Verstat header field in the INVITE request.

7 Architecture

This clause shows functional elements involved in originating, routing, and terminating emergency calls and used for location acquisition and conveyance, and caller identity authentication and SIP RPH signing.

This document re-uses functional elements as defined in 3GPP TS 23.167 [Ref 1], and where appropriate, shows their interconnection with NENA i3 elements. While some NGCS elements within the ESInet are included (mostly those which are visible to origination networks and devices or need to be shown for the reader's understanding), internal ESInet/NGCS details are only minimally described.

7.1 Overview

Figure 7.1 contains an illustration of the IMS origination network emergency call architecture provided in 3GPP TS 23.167 [Ref 1].

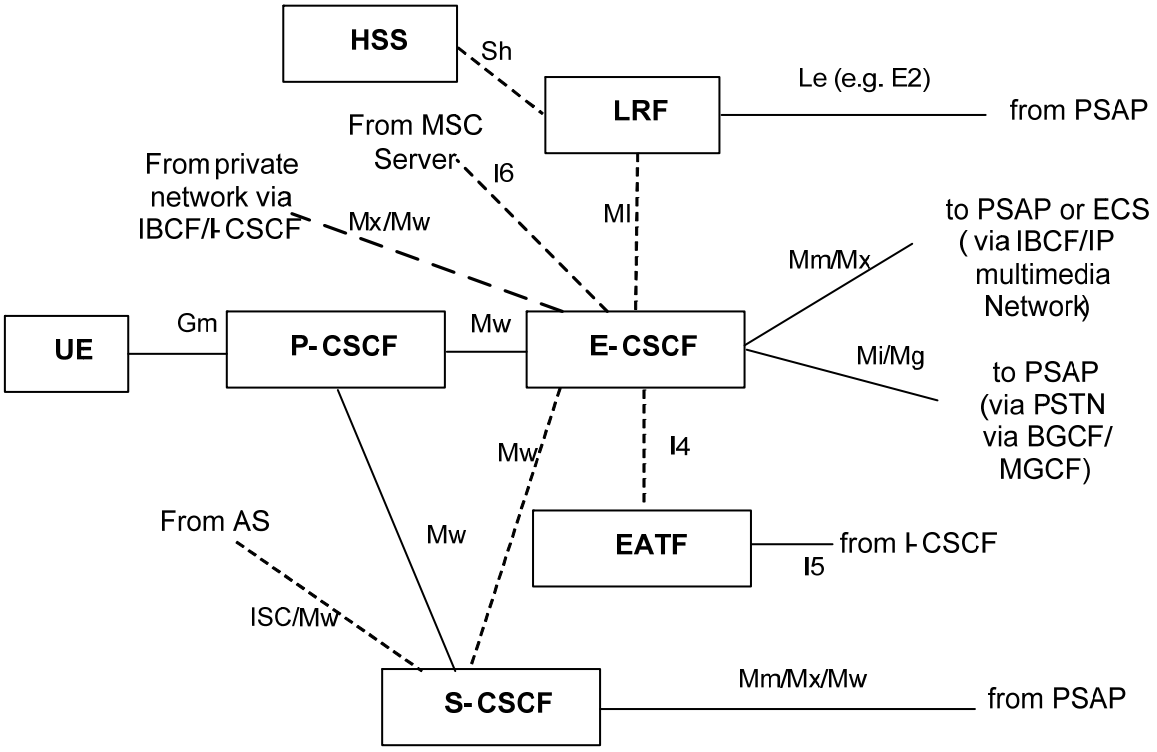

Figure 7.1 – IMS origination network emergency call architecture from 3GPP TS 23.167

For a more complete architectural view, see 3GPP TS 23.002 [Ref 4].

Error! Reference source not found. illustrates an expanded architecture that takes into account the network elements of NENA's i3 architecture and legacy emergency services network. Except for the IMS network interfaces to the emergency services network, the emergency services network architecture is out of scope and is shown for informational purposes. For simplicity, the Common IMS Network shown does not include all IMS network elements from Figure 7.1. The Common IMS Network supports a variety of access types with mobile, nomadic, or fixed user equipment. The Common IMS Network delivers each call to either a legacy emergency services network or a NENA i3 ESInet. Calls destined for a legacy emergency services network are delivered from a Media Gateway Control Function (MGCF) to a Selective Router.

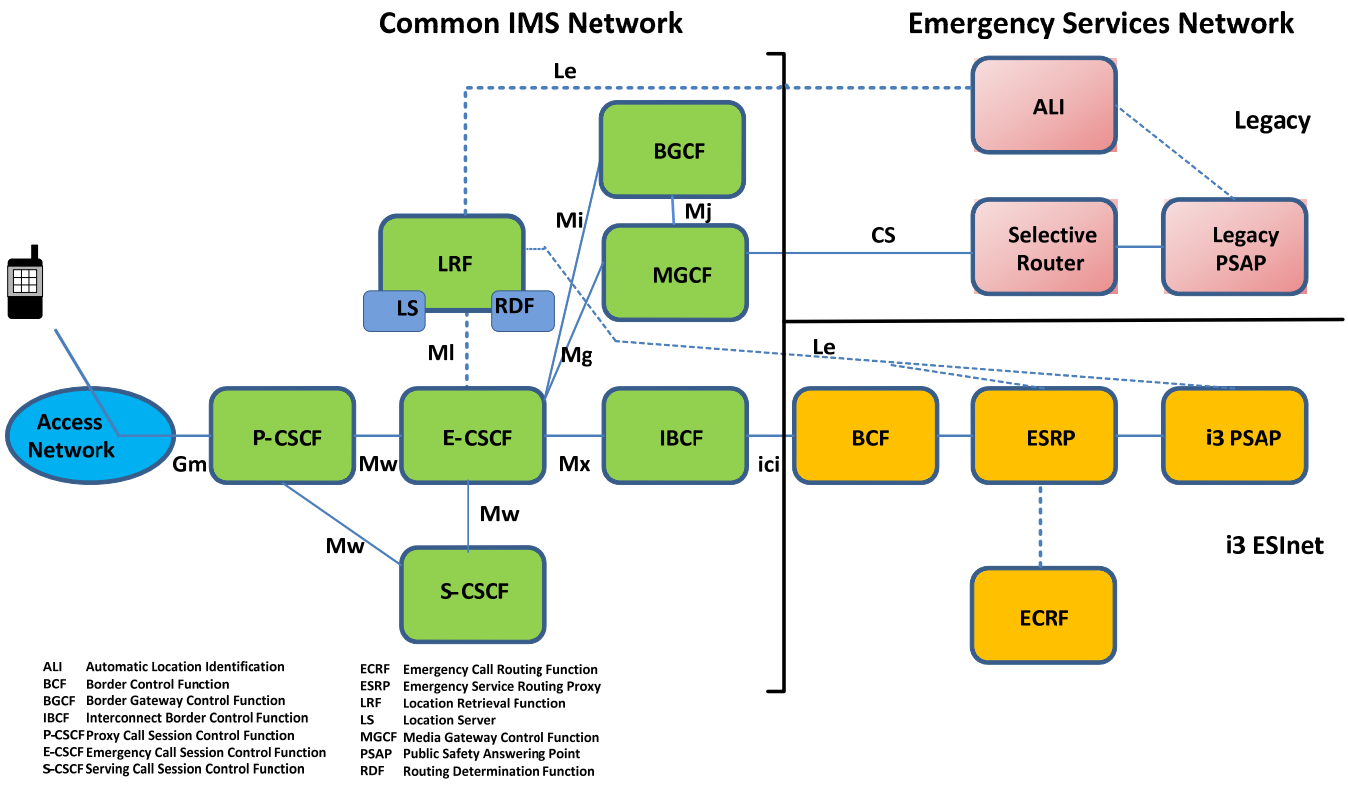

Figure 7.2 - Expanded Architecture

In the North American architecture, the emphasis is on the relationship between the originating IMS network and the interconnected emergency services network, rather than the PSAP. For example, emergency calls destined for legacy PSAPs may be directed from the originating IMS network to a Selective Router in a legacy emergency services network or to an Emergency Services IP Network (ESInet) that hosts legacy PSAPs. Emergency calls destined for IP-capable PSAPs are directed from the originating IMS network to an ESInet. Thus, in North America, it is the capabilities of the interconnected emergency services network that influence call handling within the IMS originating network, rather than the specific capabilities of the PSAP to which the call will ultimately be delivered.

For calls to a NENA i3 ESInet, calls may be delivered with the location of the caller (location-by-value [LbyV]) or a location URI (location-by-reference [LbyR]) using a Reference Identifier that the ESInet may use to query the Common IMS Network for the location. The IMS network may be queried both during call set up and after the call has reached the PSAP.

If the Common IMS Network needs to acquire the location it may do so via an LS. The characteristics of the LS may differ based upon the class of service. For example, for mobile calls, the Common IMS Network may query location determination equipment via the LS.

Once the Common IMS Network has location, it must select the appropriate emergency services network to deliver the call to. The LRF may use internal processes to access an integrated RDF to do this or it may interrogate an external RDF.

Emergency calls may be delivered either to a NENA i3 ESInet, or to a legacy Selective Router. These cases are illustrated in more detail in Clause 8.2, *Call Flows*.

Figure 7.3 illustrates a reference architecture that supports caller identity authentication and SIP RPH signing in the context of emergency calls that are routed via an i3 ESInet/NGCS. This architecture builds on the calling number authentication/verification architecture supported by 3GPP TS 24.229 and TS 23.228, where an IBCF in an originating IMS network, if configured through operator policies, invokes an Application Server referred to in Figure 7.3 as a Secure Telephone Identity Authentication Service (STI-AS), via the Ms reference point for the signing and attestation of caller identity information and the signing of RPH, if available in an incoming request. The IBCF then includes the signed information in the outgoing request. Although out of scope for this document,

Figure 7.3 also shows verification of caller identity and RPH in an i3 ESInet/NGCS by having the Emergency Service Routing Proxy (ESRP) interact with a Secure Telephone Identity Verification Service (STI-VS).

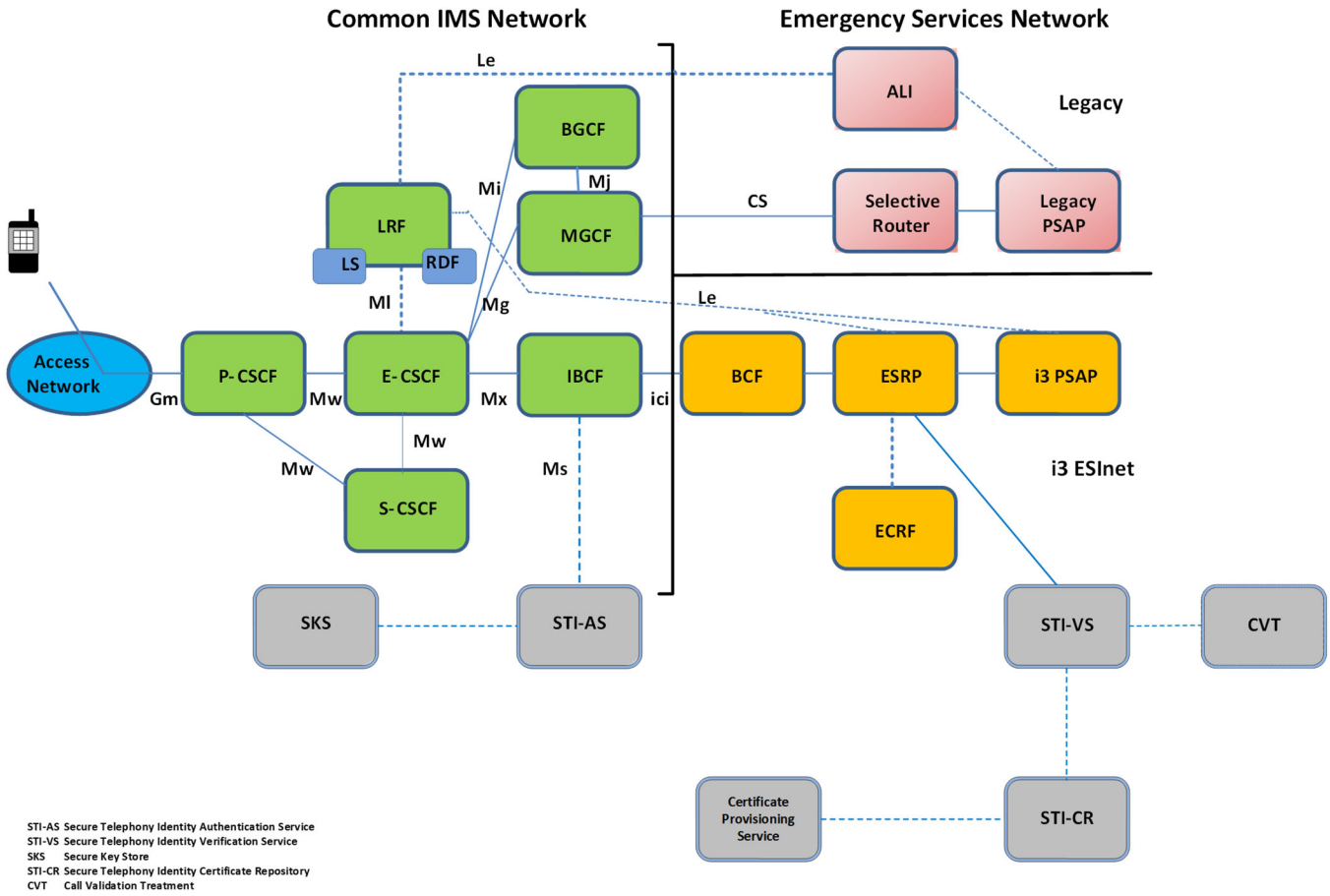

Figure 7.3 - Emergency Call - Caller Identity Authentication and RPH Signing Architecture

Based on the architecture illustrated in Figure 7.3, the Proxy Call Session Control Function (P-CSCF) receives the emergency call from the User Equipment via the Access Network. The P-CSCF detects that the call is an emergency call and forwards it to/toward the E-CSCF. The P-CSCF may populate attestation information associated with the caller identity as well as the RPH information in the outgoing signaling to the E-CSCF. The E-CSCF receives the emergency call from the P-CSCF and interacts with a Location Retrieval Function (LRF) to obtain location and routing information for the call. The LRF obtains location information associated with the emergency call (by interacting with an LS, if necessary) and uses that location to acquire routing information for the emergency call from the RDF. The LRF returns location and routing information to the E-CSCF. The E-CSCF then forwards the emergency call based on the routing information. If the call is to be routed via an NG9-1-1 Emergency Services Network (i.e., i3 ESInet), the E-CSCF passes the call to an IBCF. The IBCF sends two signing requests to the STI-AS: one associated with the caller identity and one associated with the RPH. The STI-AS determines, through service provider-specific means, the legitimacy of the content of the caller identity and the RPH information sent to it in the signing request. The STI-AS then securely requests its private key from the Secure Key Store (SKS). The SKS returns the private key to the STI-AS and the STI-AS uses it to sign the caller identity and RPH information. The STI-AS then returns two signing responses to the IBCF, one containing an identityHeader parameter associated with the signed caller identity and one containing an identityHeader parameter associated with the signed RPH. The IBCF then uses the identityHeader parameters to populate Identity header fields in the outgoing SIP INVITE message that it sends to the i3 ESInet/NGCS.

When the ESRP in the i3 ESInet receives the emergency call, it passes the SIP INVITE message associated with the call to the STI-VS. The STI-VS verifies the signatures in the Identity header fields, which validate the signature used when the caller identity and RPH field were signed. The STI-VS may interact with the Call Validation Treatment (CVT) based on local policy and agreements between the 9-1-1 Authority and the analytics/CVT provider. The CVT is an optional function that can be invoked to perform call analytics or other spam mitigation techniques. The STI-

VS passes the SIP INVITE message back to the ESRP, including an indication of the results of the verification process (i.e., a “verstatValue parameter associated with the verified caller identity and a “verstatPriority” parameter associated with the verified RPH). The ESRP proceeds with normal emergency call handling, using location information associated with the emergency call to query an Emergency Call Routing Function (ECRF) and using the routing information returned by the ECRF to pass the call forward [via a Border Control Function (BCF)] to the i3 PSAP. The emergency call is delivered to the i3 PSAP Call Handling functionality with the caller identity (i.e., callback) information and associated attestation level and verification results, as well as location information and the RPH (and associated verification results).

7.2 IMS Functional Elements

7.2.1 User Equipment (UE)

User Equipment is used here as defined in 3GPP TS 23.167 [Ref 1].

The UE initiates the emergency session establishment request.

7.2.2 Proxy Call Session Control Function (P-CSCF)

The Proxy Call Session Control Function is used here as defined in 3GPP TS 23.167 [Ref 1], and includes functionality defined in Release 17 of 3GPP TS 24.229 [Ref 2].

The P-CSCF receives the emergency session establishment request from the UE, detects that it is an emergency session request, and forwards it to the E-CSCF. Based on the operator policy, in some situations the P-CSCF may forward the emergency session establishment request to the S-CSCF.

7.2.3 Emergency Call Session Control Function (E-CSCF)

The Emergency Call Session Control Function is used here as defined in 3GPP TS 23.167 [Ref 1].

The E-CSCF receives the emergency session establishment request from the P-CSCF, obtains location information, obtains routing information, and forwards the emergency session establishment request per the routing information.

> NOTE: In some situations where the P-CSCF has forwarded the SIP INVITE to S-CSCF, the E-CSCF will receive the emergency session establishment request from S-CSCF. Also, when session continuity is supported, the E-CSCF will forward the SIP INVITE to the EATF and provide the above functions upon receiving the SIP INVITE back from the EATF.

7.2.4 Serving Call Session Control Function (S-CSCF)

The Serving Call Session Control Function is used here as defined in 3GPP TS 23.167 [Ref 1].

7.2.5 Location Retrieval Function (LRF)

The Location Retrieval Function (LRF) is used here as defined in 3GPP TS 23.167 [Ref 1] and its functionality is expanded within this standard.

The LRF retrieves location information for a UE and obtains routing information for an emergency session of the UE from the Routing Determination Function (RDF).

7.2.6 Routing Determination Function (RDF)

The Routing Determination Function (RDF) is used here as defined in 3GPP TS 23.167 [Ref 1] and its functionality is expanded within this standard.

The RDF provides routing information for an emergency session.

7.2.7 Media Gateway Control Function (MGCF)

The Media Gateway Control Function (MGCF) is used here as defined in 3GPP TS 23.167 [Ref 1] and expanded in Clause 8.5.5 of this standard.

7.2.8 Emergency Access Transfer Function (EATF)

The Emergency Access Transfer Function (EATF) is used here as defined in 3GPP TS 23.167 [Ref 1].

The EATF supports session continuity (e.g., Handover) of an emergency call initially established using IMS when movement of the UE requires a change of access network from packet network (e.g., LTE) to circuit network [e.g., Global System for Mobile communications (GSM) or Universal Mobile Telecommunications System (UMTS)].

7.2.9 Interrogating Call Session Control Function (I-CSCF)

The Interrogating Call Session Control Function is used here as defined in 3GPP TS 23.167 [Ref 1].

7.2.10 Location Server (LS)

The Location Server is used here as defined in 3GPP TS 23.167 [Ref 1].

7.2.11 Breakout Gateway Control Function (BGCF)

The Breakout Gateway Control Function (BGCF) is used here as defined in 3GPP TS 23.228 [Ref 34].

7.2.12 Interconnection Border Control Function (IBCF)

The Interconnection Border Control Function (IBCF) is used here as defined in 3GPP TS 23.228 [Ref 34], and includes functionality defined in Release 17 of 3GPP TS 24.229 [Ref 2].

7.2.13 Home Subscriber Server (HSS)

The Home Subscriber Server (HSS) is used here as defined in 3GPP TS 23.167 [Ref 1].

7.3 Emergency Services Network Functional Elements

7.3.1 Automatic Location Identification (ALI)

This term (most often used as an acronym) is used to refer to a location database, and the mechanisms for populating and accessing the database and for associating a call with the caller's location. For fixed access, the database is pre-populated with the MSAG-validated civic address associated with the service. For mobile access, the database is dynamically populated with a temporary record. See *NENA Standard Data Formats for E9-1-1 Data Exchange & GIS Mapping*, [Ref 101] for further details.

7.3.2 Border Control Function (BCF)

The Border Control Function (BCF) is used here as defined in NENA i3 [Ref 100].

The BCF controls all traffic into and out of an ESInet. Normally, originating networks have secure private (or virtual private) connections to commonly used ESInets, but these do not bypass the BCF.

7.3.3 Emergency Service Routing Proxy (ESRP)

The Emergency Service Routing Proxy (ESRP) is used here as defined in NENA i3 [Ref 100].

The ESRP acts as a SIP proxy within the ESInet, somewhat analogous to an E-CSCF in the originating network.

7.3.4 Emergency Call Routing Function (ECRF)

The Emergency Call Routing Function (ECRF) is used here as defined in NENA i3 [Ref 100].

The ECRF may be queried to learn how to route an emergency call.

7.3.5 Public Safety Answering Point (PSAP)

The Public Safety Answering Point (PSAP) can be either a legacy PSAP or NENA i3 PSAP.

For legacy PSAPs, the call is delivered, typically via a Multi-Frequency (MF) interface, and the PSAP must query for location. The NENA i3 PSAP is a SIP end point (client) within or connected through the ESInet. The NENA i3 PSAP may either receive location information in the call request or may have to query for location. The human call taker at the PSAP communicates with the originating user.

7.3.6 Selective Router (SR)

A Selective Router (also known as a Legacy Selective Router, Enhanced 9-1-1 Control Office, or 9-1-1 Selective Routing Tandem), routes emergency calls to the appropriate PSAP. See *NENA Master Glossary of 9-1-1 Terminology* [Ref 101] for further details.

7.4 Functional Elements Supporting Caller Identity Authentication/Verification and RPH Signing/Verification

This clause describes the functional elements that support caller identity authentication/verification and RPH signing/verification in the context of emergency calls. This clause also highlights additional functionality required of some of the IMS and i3 functional elements described in Clauses 7.2 and 7.3 to support caller authentication/verification and RPH signing/verification for emergency calls.

7.4.1 P-CSCF

As described in Clause 7.2.2, the P-CSCF receives the emergency session establishment request from the UE, detects that it is an emergency session request, and forwards it to the E-CSCF. A P-CSCF operating in an Originating Service Provider network that supports calling number authentication and RPH signing may, based on local policy, be responsible for inserting attestation information related to the asserted caller identity and populating the RPH in a SIP INVITE associated with an emergency origination. Based on local policy, if the P-CSCF is responsible for providing attestation information on the caller identity associated with an authenticated emergency call, the P-CSCF will also insert a “verstat” parameter in the P-Asserted-Identity header and an origination identifier in an Origination-Id header field of the outgoing SIP INVITE message. As described in Clause 5.2.1 of 3GPP TS 24.229 [Ref 2], where the originating network uses the RPH field to control the priority of emergency calls, the P-CSCF shall add a Resource-Priority header field containing a namespace of "esnet" as defined in RFC 7135 [Ref 53]. For emergency calls in North America, the P-CSCF will populate a value of “esnet.1” in the RPH.

7.4.2 IBCF

In the context of an emergency call from an authenticated user handled by an originating IMS network that supports caller authentication and RPH signing, an exit IBCF that supports the Ms reference point shall interact with the STI-AS to request authentication/signing of the caller identity and RPH. Upon receiving a response from the STI-AS, the exit IBCF will populate Identity header fields in the outgoing SIP INVITE message based on the content of the response. The exit IBCF will also remove the “verstat” from the From header or P-Asserted-Identity header prior to sending the SIP INVITE over the IP NNI to i3 ESInet.

7.4.3 Secure Telephone Identity Authentication Service (STI-AS)

The STI-AS is a SIP application server that performs the function of the authentication service defined in RFC 8224 [Ref 50]. It should either itself be highly secured and contain the Secure Key Store (SKS) of secret private key(s) or have an authenticated, Transport Layer Security (TLS)-encrypted interface to the SKS that stores the secret private key(s) used to create PASSporT signatures.

In the context of emergency calls, the STI-AS receives signing requests from an exit IBCF then determines, through service provider-specific means, the legitimacy of the content of the caller identity and the RPH field. The STI-AS then securely requests its private key from the SKS. Upon receiving the private key from the SKS, the STI-AS signs and returns to the IBCF an identityHeader parameter associated with the caller identity and an identityHeader parameter associated with the RPH.

7.4.4 Secure Telephone Identity Verification Service (STI-VS)

The STI-VS is a SIP application server that performs the function of the verification service defined in RFC 8224 [Ref 50]. Upon receiving a SIP INVITE message containing Identity headers associated with an emergency call from an ESRP in the i3 ESInet, the STI-VS will use a Hypertext Transfer Protocol Secure (HTTPS) interface to the Secure Telephone Identity Certificate Repository (STI-CR) that is referenced in the Identity header field to retrieve the provider public key certificate. The STI-VS validates the PASSporT information provided in the Identity headers contained in the SIP INVITE message and includes verification status information associated with the caller identity (i.e., a “verstat” tel uri parameter in the P-Asserted-Identity header field, or the From header field, if no P-Asserted-Identity header field is present), and with the RPH (in a Priority-Verstat header field) in the SIP INVITE message returned to the ESRP to convey the results of the verification service.

7.4.5 Call Validation Treatment (CVT)

This CVT is a logical function that could be an application server function or a third party application for applying anti-spoofing mitigation techniques once the signature is positively or negatively verified. The CVT interacts with the STI-VS and provides information that may influence how the results of the verification should be displayed to the called user.

7.4.6 Secure Key Store (SKS)

The Secure Key Store is a logical highly secure element that stores secret private key(s) that can be accessed by the authentication service (STI-AS).

7.4.7 Certificate Provisioning Service

The Certificate Provisioning Service is a logical service used to provision certificate(s) used for STI.

7.4.8 Secure Telephone Identity Certificate Repository (STI-CR)

The STI-CR represents the publicly accessible store for public key certificates. The STI-CR should provide an HTTPS web service that can be validated back to the owner of the public key certificate.

7.4.9 ESRP

As described in Clause 7.3.3, the ESRP is an i3 functional element which is a SIP proxy server that selects the next hop routing within the ESInet based on location and policy. In the context of caller identity authentication/verification and RPH signing/verification for 9-1-1 calls, the ESRP is responsible for interacting with the STI-VS for verification of the signatures associated with the caller identity information and RPH information provided in the verification request. The ESRP is expected to pass the received SIP INVITE message to the verification service before applying any call processing (e.g., location- and/or policy-based routing) to the call.

7.5 High Level Signaling Flow Diagram

This clause provides a high-level signaling flow diagram to illustrate the establishment of an emergency call originated in an IMS network. The signaling flow illustrates that the IMS originating network receives the emergency call request in a SIP INVITE from the UE and, after determining the emergency routing information, routes the call to the PSAP through the MGCF/SR or through the ESInet. The call flows that illustrate the various cases of emergency call handling are illustrated in Clause 8.2.

Figure 7.4 provides a high level signaling flow diagram in establishing an emergency call towards a PSAP.

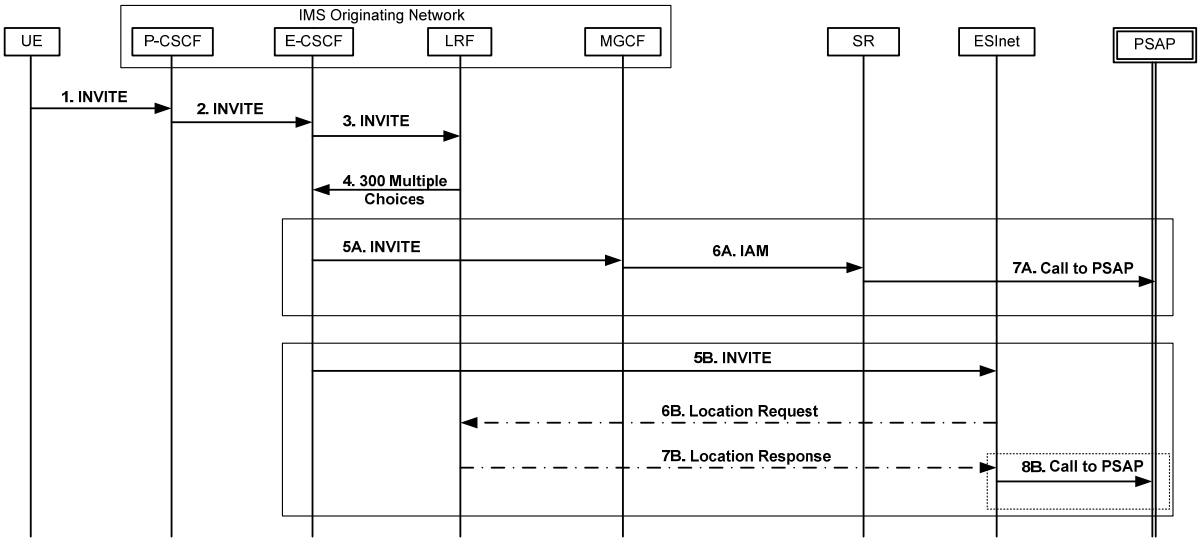

Figure 7.4 – A High Level Signaling Flow Diagram

Step 1. The UE sends the SIP INVITE to the P-CSCF.

Step 2. The P-CSCF forwards the SIP INVITE to the E-CSCF. See Note 1.

Step 3. The E-CSCF forwards the SIP INVITE to the LRF. See Note 2.

Step 4. The LRF returns the emergency call routing information to the E-CSCF in a SIP 300 Multiple Choices.

Step 5A. If the call is destined to a legacy emergency services network, the E-CSCF constructs a SIP INVITE using the information received from the LRF and forwards the SIP INVITE towards the MGCF via a BGCF (not shown).

Step 6A. The MGCF maps the SIP INVITE to an ISUP IAM and forwards the ISUP IAM to the SR. Alternatively; the MGCF through the MGW could use MF signaling towards the SR.

Step 7A. The SR offers the call to the PSAP.

Step 5B. If the call is destined to a NENA i3 emergency services network, the E-CSCF constructs a SIP INVITE using the information received from the LRF and forwards the SIP INVITE towards the ESInet via IBCF (not shown).

Step 6B. The ESRP (not shown) in the ESInet may query the LRF for the UE location information for emergency routing purposes.

Step 7B. The LRF returns the UE location information when queried by the ESRP.

Step 8B. The ESInet forwards the call to the PSAP.

NOTE 1: Alternatively, based on operator policy, the SIP INVITE may be forwarded through the S-CSCF to the E-CSCF, as specified in 3GPP TS 24.229 [Ref 2].

NOTE 2: If operator policy supports session continuity, the E-CSCF forwards the SIP INVITE to the EATF, which then forwards the SIP INVITE back to the E-CSCF, as specified in 3GPP TS 24.229 [Ref 2] and 3GPP TS 24.237 [Ref 27].

7.6 Adding or Dropping Media to an Existing Voice Call

In support of a multimedia emergency call, it is possible to add media during the conversation. For example, while the caller and the Telecommunicator are talking, the caller may indicate he/she has additional media (picture, video clip, etc.). If the PSAP equipment is capable of receiving that type of media, the Telecommunicator may ask the caller to forward it. To do this, a session reinvite is sent to include the additional media. A session reinvite is used in a similar manner to drop media (not shown).

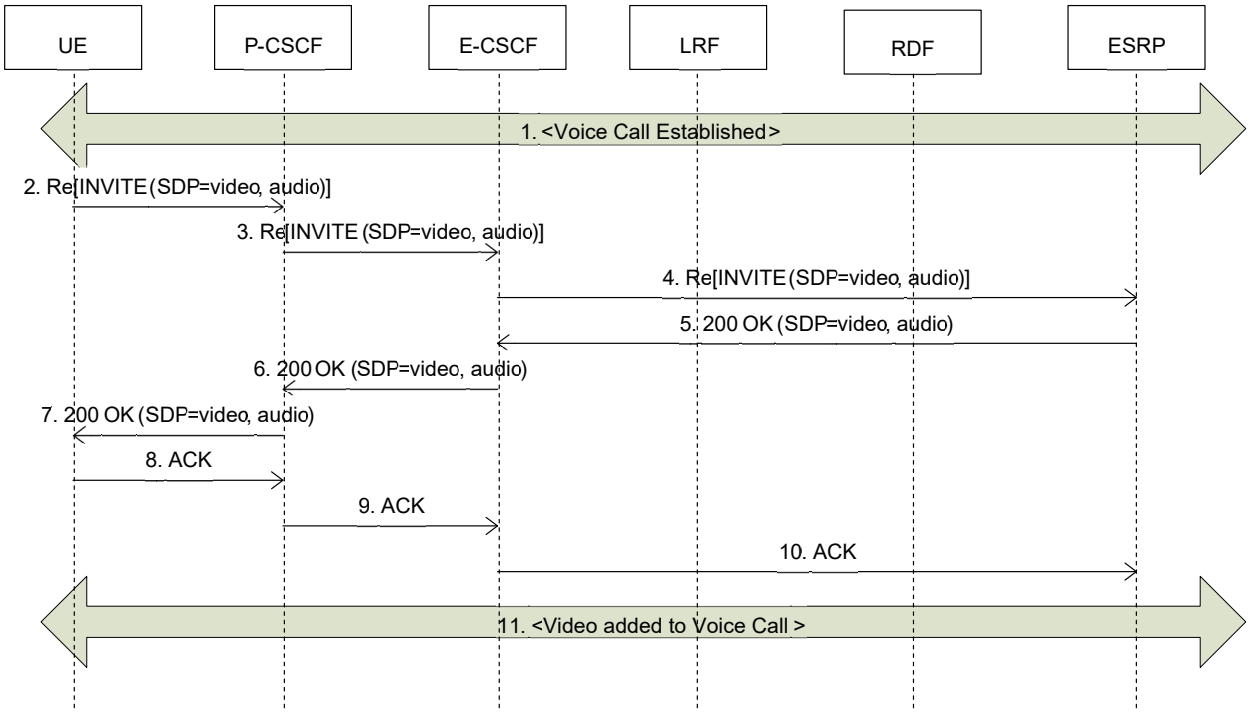

Figure 7.5 – Adding Media to an Existing Voice Call

Step 1. An existing voice call is established, and the caller tries to send a video clip of the incident.

Step 2. The UE sends a SIP re-INVITE or SIP UPDATE (not shown) to the P-CSCF that contains the additional media information (i.e., SDP with audio and video).

Step 3. The P-CSCF interacts with the access network to initiate the steps to reserve resources for video transmission and then forwards the SIP re-INVITE or SIP UPDATE (not shown) to the E-CSCF.

Step 4. The E-CSCF forwards the SIP re-INVITE or SIP UPDATE (not shown) to the ESRP which in turn forwards the SIP re-INVITE or SIP UPDATE to the NG9-1-1 PSAP (not shown).

Step 5. The NG9-1-1 PSAP sends the SIP 200 OK to the ESRP, which in turn forwards the SIP 200 OK to the E-CSCF. The SIP 200 OK indicates that the NG9-1-1 PSAP has accepted the additional media information (i.e., the SDP answer for audio and video).

Step 6. The E-CSCF forwards the SIP 200 OK back to the P-CSCF.

Step 7. The P-CSCF interacts with the access network to complete the steps of reserving the resources for video transmission (not shown) and then forwards the SIP 200 OK back to the UE.

The following steps are applicable only for the SIP re-INVITE case (i.e., not for the SIP UPDATE case):

Step 8. The UE sends the SIP ACK.

Step 9. The P-CSCF forwards the SIP ACK.

Step 10. The E-CSCF forwards the SIP ACK.

Step 11. The additional media for audio and video is established.

7.7 Procedures Related to Establishment of IMS Emergency Session

7.7.1 SOS Service URNs

When a user calls 9-1-1, the generic sos service urn defined in RFC 5031 [Ref 41] will be sent by the UE to indicate an emergency call. However, all sos sub-services will also be considered an emergency call. The sos service urn is passed through to the ESInet unaltered.

7.8 MMES (audio and video) Call to Legacy PSAP via Legacy SR

This call flow illustrates a scenario where a calling party originates a call with the media type Audio and Video. The call flow does not show all the steps involved in an emergency call handling (e.g., it does not show all the SIP messages, it does not show the LRF subscribing to call status events etc.). The focus here is the media.

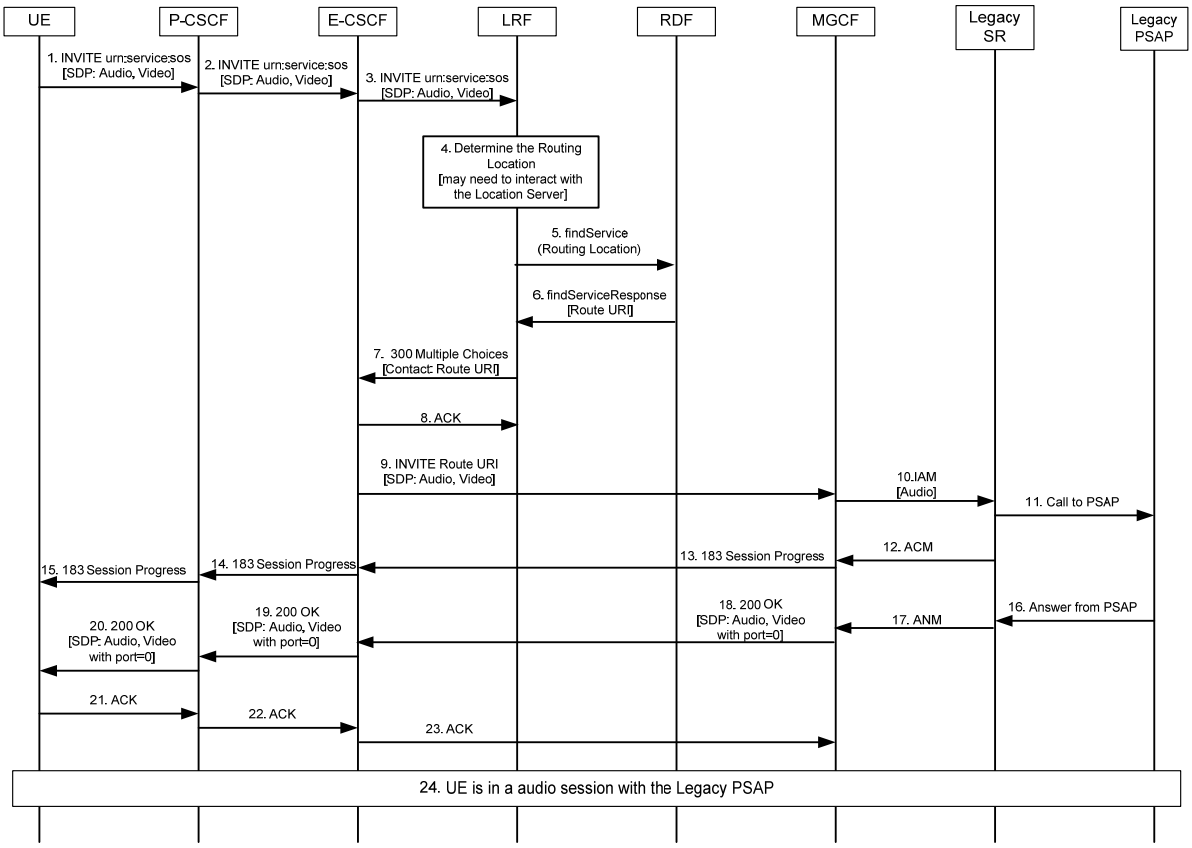

Figure 7.6 – MMES (audio and video) Call to Legacy PSAP via Legacy SR

Step 1. UE sends a SIP INVITE to the P-CSCF with media types in the SDP showing Audio and Video.

Step 2. P-CSCF forwards the SIP INVITE to the E-CSCF. There is no change in the handling of SIP INVITE at the P-CSCF as far as media type is concerned.

Step 3. E-CSCF forwards the SIP INVITE to the LRF. There is no change in the handling of SIP INVITE at the E-CSCF as far as media type is concerned.

Step 4. As it is done for any emergency call, the LRF determines the Routing Location to be used to find the PSAP routing information. For this, the LRF may interact with the LS.

Step 5. The LRF sends the LoST: findService message with Routing Location as the key to the RDF to acquire the routing information.

Step 6. The RDF determines the routing information (shown as Route URI) based on the Routing Location and returns the same to the LRF in the LoST: findServiceResponse message. The LoST: findServiceResponse message contains the Route URI.

Step 7. The LRF constructs a SIP 300 Multiple Choices with the routing information (only the Route URI is shown in this flow) coded into the Contact header and returns the SIP 300 Multiple Choices to the E-CSCF.

Step 8. The E-CSCF returns a SIP ACK to the LRF completing the E-CSCF-to-LRF transaction.

Step 9. The E-CSCF examines the format of the Route URI and determines that, in this particular example, the Route URI points to the Legacy SR. The E-CSCF constructs the SIP INVITE populating the content of the Route URI in the Request URI and forwards the SIP INVITE towards the MGCF (through the BGCF, not shown).

Step 10. MGCF is aware of the fact that it cannot support the Video, but since it can support the Audio, it constructs and sends an ISUP: IAM message towards the Legacy SR. As described elsewhere in the document, MGCF may also use MF signaling (not shown in the flow) in establishing the call toward Legacy SR.

Step 11. Legacy SR determines the PSAP and offers the call to that PSAP (Legacy PSAP).

Step 12. As a part of the ISUP signaling protocol, the Legacy SR returns ISUP: ACM to the MGCF.

Step 13. MGCF sends a SIP 183 Session Progress towards the E-CSCF (through the BGCF, not shown).

Step 14. E-CSCF forwards the SIP 183 Session Progress to the P-CSCF.

Step 15. P-CSCF forwards the SIP 183 Session Progress to the UE.

Step 16. Legacy PSAP answers the call.

Step 17. Legacy SR sends an ISUP: ANM to the MGCF.

Step 18. MGCF sends a SIP 200 OK with the SDP Answer information towards the E-CSCF (through BGCF, not shown). Since Video is not supported, the MGCF includes the information for Audio and rejects the Video offer by setting the port = 0.

Step 19. E-CSCF forwards the SIP 200 OK to the P-CSCF.

Step 20. P-CSCF forwards the SIP 200 OK to the UE. UE now understands that Video was rejected and continues processing the call with Audio as the only media type.

Step 21. UE returns the SIP ACK to the P-CSCF.

Step 22. P-CSCF forwards the SIP ACK to the E-CSCF.

Step 23. E-CSCF sends the SIP ACK to the MGCF.

Step 24. The UE is in an audio session with the Legacy PSAP.

7.9 MMES Upgrade Attempt of an Emergency Call with Legacy PSAP

This call flow illustrates a scenario where a calling party while on an audio session with a Legacy PSAP attempts to upgrade the session to an MMES session. The MGCF turns down the upgrade offer as it cannot support the MMES media types.

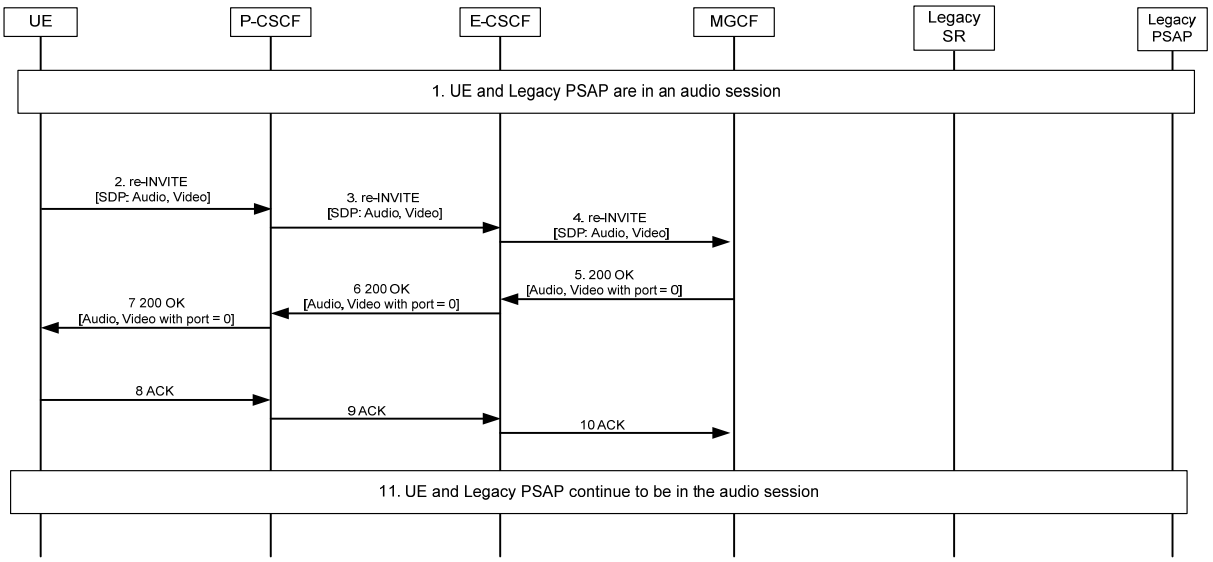

Figure 7.7 – MMES Upgrade Attempt of an Emergency Call with Legacy PSAP

Step 1. UE and Legacy PSAP are in an audio session.

Step 2. UE attempts to upgrade the session to an MMES session by sending a SIP re-INVITE or a SIP UPDATE (not shown) with the MMES media types included in the SDP. In this example, the UE includes Audio and Video as the media types.

Step 3. P-CSCF forwards the SIP re-INVITE or SIP UPDATE (not shown) to the E-CSCF.

Step 4. E-CSCF forwards the SIP re-INVITE or UPDATE (not shown) to the MGCF to the LRF. Note that the BGCF is not the signaling path.

Step 5. MGCF cannot support the Video, but it can the Audio and hence, sends a SIP 200 OK to the E-CSCF with the SDP answer carrying the port=0 for the Video part.

Step 6. E-CSCF forwards the SIP 200 OK to the P-CSCF.

Step 7. P-CSCF forwards the SIP 200 OK to the UE.

Step 8. UE returns a SIP ACK to the P-CSCF.

Step 9. P-CSCF forwards the SIP ACK to the E-CSCF.

Step 10. E-CSCF forwards the SIP ACK to the MGCF.

Step 11. UE and Legacy continue to be on the audio session.

7.10 MMES (without an offer of audio or text media) Call to Legacy PSAP via Legacy SR

This call flow illustrates a scenario where a calling party originates a call that is destined for a Legacy PSAP with a media type that is not supported by the Legacy PSAP. The call flow does not show all the steps involved in an emergency call handling (e.g., it does not show all the SIP messages, it does not show the LRF subscribing to call status events etc.). The focus here is the media. Due to its size, the flow is split into two figures [Figure 7.7 and Figure 7.8]. Those two figures together have to be read as one flow.

This scenario assumes that the UE is able to initiate a subset of the media indicated in the 488 Not Acceptable Here (audio or text). This scenario also assumes that the MGCF is able to return 488 Not Acceptable Here with the media types supported by the media gateway when the SDP in the SIP INVITE contains media types not supported by the media gateway.

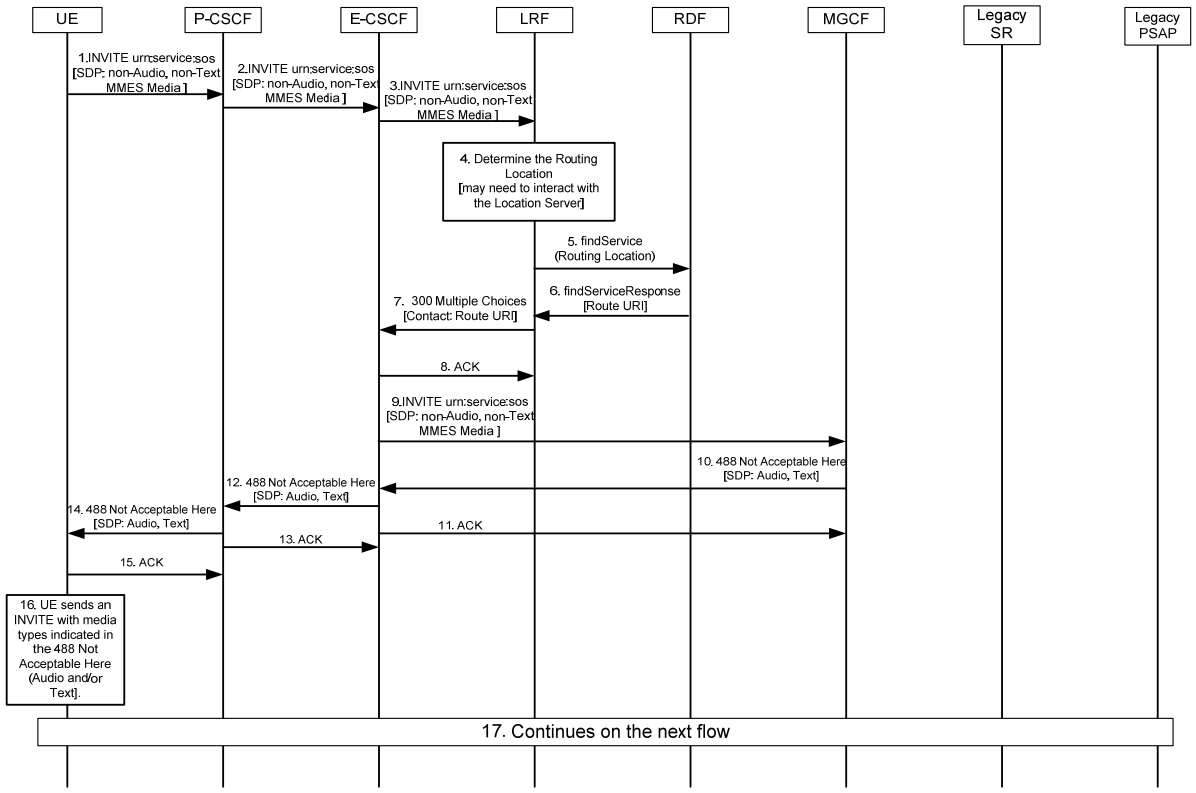

Figure 7.7 – MMES (w/o audio or text) Call to Legacy PSAP via Legacy SR (flow 1 of 2)

Step 1. UE sends a SIP INVITE to the P-CSCF with media types in the SDP showing an MMES media type that is neither Audio nor Text.

Step 2. P-CSCF forwards the SIP INVITE to the E-CSCF. There is no change in the handling of SIP INVITE at the P-CSCF as far as media type is concerned.

Step 3. E-CSCF forwards the SIP INVITE to the LRF. There is no change in the handling of SIP INVITE at the E-CSCF as far as media type is concerned.

Step 4. As is done for any emergency call, the LRF determines the Routing Location to be used to find the PSAP routing information. For this, the LRF may interact with the LS.

Step 5. The LRF sends the LoST: findService message with Routing Location as the key to the RDF to acquire the routing information.

Step 6. The RDF determines the routing information (shown as Route URI) based on the Routing Location and returns it to the LRF in the LoST: findServiceResponse message. The LoST: findServiceResponse message contains the Route URI.

Step 7. The LRF constructs a SIP 300 Multiple Choices with the routing information (only the Route URI is shown in this flow) coded into the Contact header and returns the SIP 300 Multiple Choices to the E-CSCF.

Step 8. The E-CSCF returns a SIP ACK to the LRF completing the E-CSCF-to-LRF transaction.

Step 9. The E-CSCF examines the format of the Route URI and determines that, in this particular example, the Route URI points to the Legacy SR. The E-CSCF constructs the SIP INVITE populating the content of the Route URI in the Request URI and forwards the SIP INVITE towards the MGCF (through the BGCF, not shown).

Step 10. MGCF determines that it does not support any of the media types contained in the SIP INVITE. Therefore, the MGCF returns a SIP 488 Not Acceptable Here towards the E-CSCF indicating the media types that it can support (in this example, it is Audio and Text).

Step 11. E-CSCF returns the SIP ACK to the MGCF to complete the transaction.

Step 12. E-CSCF forwards the SIP 488 Not Acceptable Here to the P-CSCF.

Step 13. P-CSCF returns the SIP ACK to the E-CSCF to complete the transaction.

Step 14. P-CSCF forwards the SIP 488 Not Acceptable Here to the UE.

Step 15. UE returns the SIP ACK to the P-CSCF to complete the transaction.

Step 16. UE that complies with the 3GPP 24.229 [Ref 2] requirements sends a SIP INVITE with a subset of the media types included in the SIP 488 Not Acceptable Here.

Step 17. The flow continues.

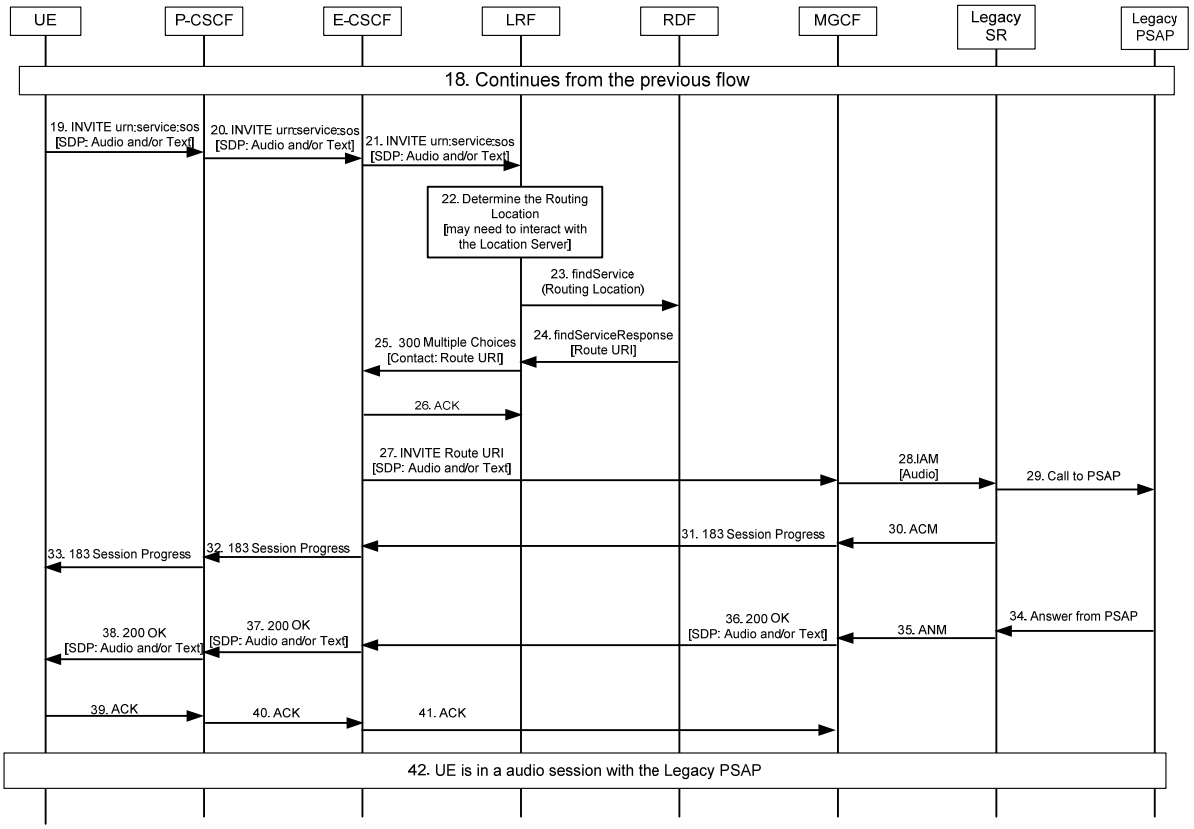

Figure 7.8 - MMES (w/o audio or text) Call to Legacy PSAP via Legacy SR (flow 2 of 2)

Step 18. The flow continues from the previous flow.

Step 19. UE re-sends a SIP INVITE to the P-CSCF with a subset of media types received as the supported media types in the SIP 488 Not Acceptable Here. In this example, the UE includes Audio and/or Text as the media type.

Step 20. P-CSCF forwards the SIP INVITE to the E-CSCF. There is no change in the handling of SIP INVITE at the P-CSCF as far as media type is concerned.

Step 21. E-CSCF forwards the SIP INVITE to the LRF. There is no change in the handling of SIP INVITE at the E-CSCF as far as media type is concerned.

Step 22. As is done for any emergency call, the LRF determines the Routing Location to be used to find the PSAP routing information. For this, the LRF may interact with the LS.

Step 23. The LRF sends the LoST: findService message with Routing Location as the key to the RDF to acquire the routing information.

Step 24. The RDF determines the routing information (shown as Route URI) based on the Routing Location and returns the same to the LRF in the LoST: findServiceResponse message. The LoST: findServiceResponse message contains the Route URI.

Step 25. The LRF constructs a SIP 300 Multiple Choices with the routing information (only the Route URI is shown in this flow) coded into the Contact header and returns the SIP 300 Multiple Choices to the E-CSCF.

Step 26. The E-CSCF returns a SIP ACK to the LRF completing the E-CSCF-to-LRF transaction.

Step 27. The E-CSCF examines the format of the Route URI and determines that, in this particular example, Route URI points to the Legacy SR. The E-CSCF constructs the SIP INVITE

populating the content of the Route URI in the Request URI and forwards the SIP INVITE towards the MGCF (through the BGCF, not shown).

Step 28. MGCF constructs and sends an ISUP: IAM message towards the Legacy SR. As described elsewhere in the document, MGCF may also use MF signaling (not shown in the flow) in establishing the call toward Legacy SR.

Step 29. Legacy SR determines the PSAP and offers the call to that PSAP (Legacy PSAP).

Step 30. As a part of the ISUP signaling protocol, the Legacy SR returns ISUP: ACM to the MGCF.

Step 31. MGCF sends a SIP 183 Session Progress towards the E-CSCF (through the BGCF, not shown).

Step 32. E-CSCF forwards the SIP 183 Session Progress to the P-CSCF.

Step 33. P-CSCF forwards the SIP 183 Session Progress to the UE.

Step 34. Legacy PSAP answers the call.

Step 35. Legacy SR sends an ISUP: ANM to the MGCF.

Step 36. MGCF sends a SIP 200 OK with the SDP Answer information towards the E-CSCF (through BGCF, not shown).

Step 37. E-CSCF forwards the SIP 200 OK to the P-CSCF.

Step 38. P-CSCF forwards the SIP 200 OK to the UE.

Step 39. UE returns the SIP ACK to the P-CSCF.

Step 40. P-CSCF forwards the SIP ACK to the E-CSCF.

Step 41. E-CSCF sends the SIP ACK to the MGCF.

Step 42. The UE is in an audio and/or text session with the Legacy PSAP.

8 Stage 3

8.1 Reference Protocols

8.1.1 Location Retrieval & Routing Functions

This clause defines the relationship among the LRF, RDF, and Location Server for use in North America.

Figure 8.1 illustrates the architecture for location acquisition and routing for emergency services. The following functional elements are illustrated:

- *Emergency Call Session Control Function (E-CSCF)* – As defined in Clause 7.2.3 of this standard.
- *Location Server (LS)* – Location Servers relate functional elements that contain location. As defined in this standard, there may be various implementations of a LS. Examples of a LS may be a Gateway Mobile Location Center (GMLC) [Ref 5], a Secure User Plane Location (SUPL) Platform (SLP) [Ref 11], a Mobile Position Center (MPC) [Ref 7], or a Fixed Location Server.
- *Location Retrieval Function (LRF)* – As defined in Clause 7.2.5 of this standard and expanded upon in this clause.
- *Routing Determination Function (RDF)* – As defined in Clause 7.2.6 of this standard and expanded upon in this clause.

Despite various standard architectures allowing differences in the composition of functional elements, this standard treats each functional element as a separable logical entity. For example, the Location Server may be physically incorporated in the LRF per 3GPP TS 23.271 [Ref 5], but that is outside the scope of this document.

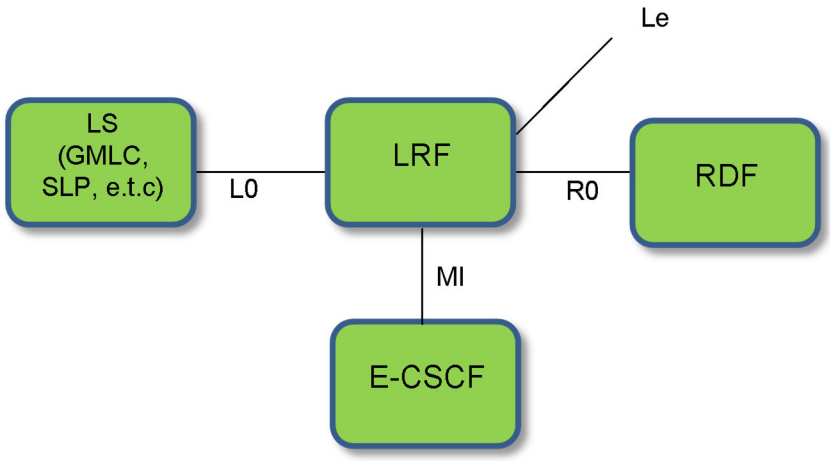

Figure 8.1 – LRF Decomposition Architecture

- *E-CSCF to LRF Reference Point (MI)*

  The MI interface is defined in 3GPP TS 23.167 [Ref 1] and expanded upon in Clauses 5.11 and 5.12 of 3GPP TS 24.229 [Ref 2]. The LRF operates as a SIP redirecting server to the E-CSCF. The E-CSCF sends a SIP INVITE to the LRF passing sufficient information in the headers and/or body to allow the LRF to determine routing (via the RDF) and acquire location if necessary. The LRF responds with a SIP 300 Multiple Choices response containing routing information and a Reference Identifier (e.g., ESRK), if necessary.

- *LRF to RDF Reference Point (R0)*

  The protocol between the LRF and the RDF is the Location to Service Translation Protocol (LoST) [Ref 6]. Using this protocol, the location and the service URN are sent to the RDF and a routing URI is returned. The LoST messages of findService and findServiceResponse are used. It is assumed that the RDF returns a SIP URI in all cases, regardless of the destination network (legacy or NENA i3 ESInet).

- *Emergency Location Client to LRF (Le)*

  3GPP TS 23.167 [Ref 1] defines the Le interface between the emergency Location Client and the LRF.

  The following protocols are allowed for the Le reference point in North America:

  - *E2 ESPOSREQ* – The E2 interface is defined in J-STD-036-C-2 [Ref 7]. The request message of ESPOSREQ and the response message of esposreq are used.
  - *Mobile Location Protocol (MLP)* – MLP is defined by OMA [Ref 8]. The Emergency Location Immediate Request (ELIR) and Emergency Location Immediate Answer (ELIA) messages are used.
  - *Dereferencing Protocol using HELD* – The IETF has defined the protocol used to deference location. The Dereferencing Protocol using HTTP Enabled Location Protocol (HELD) [Ref 9] messages of locationRequest and locationResponse are used.
  - SIP SUBSCRIBE/NOTIFY is defined by IETF [Ref 32]

- *L0 Reference Point*

  The L0 Reference Point is specific to location acquisition (initial and updated) and location continuity in mobile networks and is defined below. The following protocols are allowed for the L0 reference point in North America:

  - *E2 ESPOSREQ* – The E2 interface is defined in J-STD-036-C-2 [Ref 7]. The request message of ESPOSREQ and the response message of esposreq are used.
  - *Mobile Location Protocol (MLP)* – MLP is defined by OMA [Ref 8]. The following messages are used:
    - Emergency Location Immediate Request (ELIR);
    - Emergency Location Immediate Answer (ELIA); and

        - Emergency Location Report (ELR).
    - *Dereferencing Protocol using HELD* – The IEFT protocol to deference location. The Dereferencing Protocol using HTTP Enabled Location Protocol (HELD) [Ref 9] messages of locationRequest and locationResponse are used.
    - *HELD with identity extensions* [Ref 10]

8.1.2 Caller Identity and Resource Priority Header/Priority Header Signing and Verification

This clause defines the reference protocols used in North America to support the signing and verification of caller identity and SIP Resource Priority Header (RPH) and Priority header information associated with emergency calls and callbacks.

3GPP TS 23.228 [Ref 34] and TS 24.229 [Ref 2] describe the use of the Ms reference point between an IBCF and an AS over which HTTP 1.1, as specified in RFC 7230 [Ref 47], is used. Specifically, Annex V of TS 24.229 [Ref 2] defines a signingRequest/signingResponse and verificationRequest/verificationResponse to support caller identity signing and verification. Note that this mechanism is also supported by ATIS-1000082 [Ref 45], where the egress IBCF in the originating network is the “Authenticator” and ESRP in the i3 ESInet is the “Verifier”.

Based on TS 24.229 [Ref 2], to get an asserted caller identity signed, the client sends an HTTP POST request towards the signing server (i.e., the STI-AS) containing a PASSporT SHAKEN object. The signingRequest includes origination (“orig”) and destination (“dest”) claims, as well as an Issued At (i.e., “iat”) claim, and an origination identifier (i.e., “origid”). The signingRequest may also include an “attest” parameter that identifies the relationship between the service provider attesting the identity and the subscriber. (According to TS 24.229 [Ref 2], the signingRequest may also include a “div” claim identifying the diverting user, if applicable.) The ability for an IBCF to include this information in a signingRequest sent to an STI-AS suggests the need for an upstream element, such as a P-CSCF in the case of an emergency call request (based on local policy), to provide attestation information associated with the caller identity, and to convey the attestation level in the SIP signaling (e.g., in an Attestation-Info header) sent to an exit IBCF. According to 3GPP TS 24.229 [Ref 2] and ATIS-1000082 [Ref 45], upon receiving an HTTP 200 (OK) response to the signingRequest, the IBCF (i.e., the Authenticator) will include the value of the "identity" claim in the response from the STI-AS in an Identity header field in the forwarded SIP request. The reference architecture illustrated in Figure 7.3 and flow described in Clause 8.2.1 of this standard illustrate the use of the Ms reference point to support caller identity as well as RPH signing associated with emergency originations. The IBCF procedures described in Clause 8.5.6 of this standard also assume the use of the Ms reference point between an exit IBCF and the STI-AS to support caller identity and RPH signing/verification.

The Ms reference point described in Annex V of 3GPP TS 24.229 [Ref 2] can be leveraged to cryptographically sign and verify the SIP RPH field in SIP INVITE messages associated with emergency (9-1-1) and callback calls and the SIP Priority header associated with callback calls using the PASSporT extension defined in IETF RFC 8443 [Ref 49], including the RPH assertion values and SIP Priority header claim described in IETF RFC 9027 **Error! Reference source not found.**[Ref 50], and the associated Secure Telephone Identity (STI) protocols defined in IETF RFC 8224 [Ref 50] and IETF RFC 8225 [Ref 48].

IETF RFC 8443 [Ref 49] defines an optional extension to the PASSporT and the associated STI mechanisms to allow cryptographic signing of the SIP RPH field which is used for communications resource prioritization. It also describes how the PASSporT extension is used in SIP signaling to convey assertions of authorization of the information in the SIP RPH field. Specifically, assertion of the information in the RPH will involve the inclusion of a “ppt” extension with an “rph” claim in the PASSporT. Based on RFC 8443 [Ref 49], a PASSporT header with the "ppt" extension will consist of the following information:

```
{
"typ":"passport",
  "ppt":"rph",
  "alg":"ES256",
  "x5u":"https://www.example.org/cert.cer"
}
```

In the context of emergency calls and callback calls, the “rph” claim will provide an assertion of the value of the SIP RPH. An example of an "rph" claim for a SIP RPH field with an “esnet.1” assertion to be used with an emergency (9-1-1) origination is provided below.

```
{
  "dest":{"uri":["urn:service:sos"]},
  "iat":1443208345,
  "orig":{"tn":"12155551212"},
   "rph":{"auth":["esnet.1"]}
}
```

In addition, IETF RFC 9027 **Error! Reference source not found.** defines a new SIP Priority Header claim ("sph") for protection of the "psap-callback" value as part of the "rph" PASSporT extension to support the security of Emergency Services Networks (i.e., i3 ESInet/NGCS) for emergency callbacks. The “sph” claim shall only be used for authorized emergency callbacks and corresponds to a SIP Priority header with the value "psap-callback”. For emergency callbacks, the "orig" claim of the "rph" PASSporT represents the PSAP telephone number. The "dest" claim contains the telephone number representing the emergency caller that is being called back. The following is an example of an "rph" claim for a SIP 'Resource-Priority' header field with an "esnet.0" assertion and an “sph” claim:

```
{
  "dest":{"tn":["12155551212"]},
  "iat":1443208345,
   "orig":{"tn":"12155551213"},
  "rph":{"auth":["esnet.0"]}
   "sph":"psap-callback"
}
```

After the PASSporT header and claims have been constructed, their signature is generated normally per the guidance in RFC 8225 [Ref 48] using the full form of PASSporT.

Enhancements to the HTTP interface used over the Ms interface to support the conveyance of the “rph” claim and associated assertion values to support caller identity and RPH signing associated with emergency call requests are being addressed in 3GPP TS 24.229 Release 17.

8.2 Call Flows

This clause shows steps taken as emergency calls are initiated, routed, and delivered to a NENA i3 ESInet or legacy Selective Router interface.

The call flows apply to all media types since they only discuss the signaling functional elements and not any media-centric functional elements. Only the media types of voice and GTT apply for calls routed to a legacy emergency services network.

8.2.1 Call Delivery to a NENA i3 ESInet

Figure 8.2 and Figure 8.3 illustrate NENA i3 ESInet termination where location-by-reference is delivered to the NENA i3 ESInet:

- Figure 8.2 illustrates routing based on location acquired by the network.
- Figure 8.3 illustrates routing based on Cell identifier.
- Figure 8.4 illustrates a NENA i3 ESInet termination where location-by-value is delivered to the NENA i3 ESInet.

- Figure 8.5 illustrates the application of caller identity and RPH signing and verification associated with an emergency call request that is delivered to a NENA i3 ESInet.

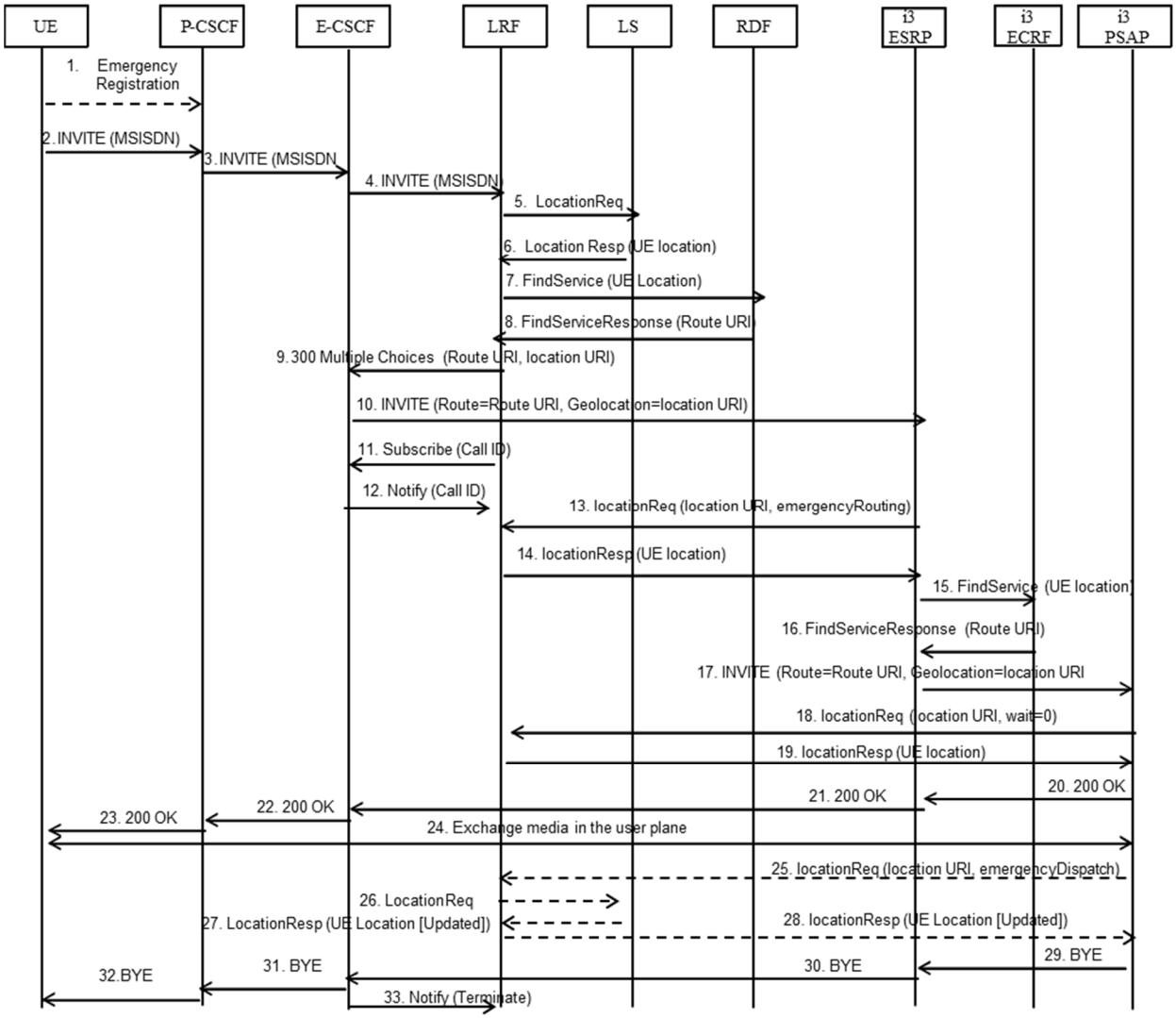

Figure 8.2 – UE Location-Routed Call Delivery to NENA i3 ESInet – Location-by-Reference

Step 1. (Conditional) Emergency registration occurs (if not already emergency registered and has credentials).

Step 2. The UE sends a SIP INVITE to the P-CSCF that contains an MSISDN and no location information.

Step 3. The P-CSCF, detecting an emergency call, forwards the SIP INVITE to the E-CSCF.

Step 4. The E-CSCF queries LRF for location and/or route, by forwarding the SIP INVITE.

Step 5. The LRF may select a technique for acquiring location information based upon the call type. The LRF interacts with the LS to acquire location/initiate position determination process.

Step 6. The LS responds with UE location value.

Step 7. The LRF queries the RDF for routing information.

Step 8. The RDF responds by providing a Route URI.

Step 9. The LRF redirects the callback to the E-CSCF with location information (in this example, location information is LbyR; therefore, the LRF constructs a Reference Identifier with the location URI) and a Route URI that will direct the call toward the ESInet.

Step 10. The E-CSCF forwards the SIP INVITE (with any location information received from the LRF; in this example, a Reference Identifier with the location URI) to the ESRP via an IBCF.

Step 11. The LRF sends a SIP SUBSCRIBE to the E-CSCF to be informed of call state. (Alternatively, the Subscription may be done at the system start-up and be applicable to all calls [not shown]).

Step 12. The E-CSCF sends an initial state NOTIFY to the LRF.

Step 13. In this example, the SIP INVITE contains a location URI, so the ESRP queries the LRF (as identified in the location URI) for location value. This call flow illustrates the use of HELD as a de-reference protocol. The value of the responseTime parameter in the HELD locationRequest sent by the ESRP is set to “emergencyRouting”.

Step 14. The LRF supplies the UE location obtained in Step 6 to the ESRP.

Step 15. (Informative) Within the ESInet, the ESRP queries the ECRF for routing information using the LoST protocol.

Step 16. (Informative) The ECRF replies to the ESRP with a PSAP URI.

Step 17. The ESRP forwards the SIP INVITE to the NENA i3 PSAP.

Step 18. In this example, the SIP INVITE contains a location URI, so the PSAP queries the LRF (as identified in the location URI) for initial location (i.e., responseTime contains a wait timer value of “0”).

Step 19. The LRF returns the UE location obtained in Step 6.

Step 20. The PSAP indicates the call has been answered by returning a SIP 200 OK to the ESRP. This Step may occur before Step 18.

Step 21. The ESRP forwards a SIP 200 OK to the E-CSCF.

Step 22. The E-CSCF forwards a SIP 200 OK to the P-CSCF.

NOTE: The E-CSCF sends a NOTIFY to the LRF based on Step 11 (not shown).

Step 23. The P-CSCF forwards a SIP 200 OK to the UE.

Step 24. Media is exchanged in the user plane.

Step 25. (Optional) The PSAP queries the LRF (as identified in the location URI) for updated location information (responseTime parameter=“emergencyDispatch” in this example).

Step 26. (Conditional on Step 25) The LRF queries the LS for updated location information. (Note that the value of the responseTime parameter [emergencyDispatch or a specific time value] will be used by the LRF to determine whether to query the LS).

Step 27. (Conditional on Step 26) The LS returns updated UE location information to the LRF.

Step 28. (Conditional on Step 25) The LRF supplies update UE location to the PSAP.

Step 29. The PSAP sends a SIP BYE to the ESRP. Note that this may be sent by the UE as well.

Step 30. The ESRP forwards a SIP BYE to the E-CSCF through the BCF/IBCF.

Step 31. The E-CSCF forwards a SIP BYE to the P-CSCF.

Step 32. The P-CSCF forwards a SIP BYE to the UE.

Step 33. The E-CSCF sends a termination SIP NOTIFY to the LRF in order to release resources. This may occur any time after step 30.

An Associated Location is used in some wireless routing scenarios where the cell address or cell centroid cannot be used to route a call to the ESInet. The Associated Location (shown as the Routing Location in the figure below) is selected by the LRF, will be used by the RDF, and is returned by the LRF to an E-CSCF based upon its request for routing location (an LbyR scenario), and may be subsequently re-used by the ESInet to route the call to the appropriate PSAP. The Associated Location is used for routing only and is not presented to the PSAP. How the Associated Location is established is beyond the scope of this standard. The procedural flow to support this is shown in the following figure.

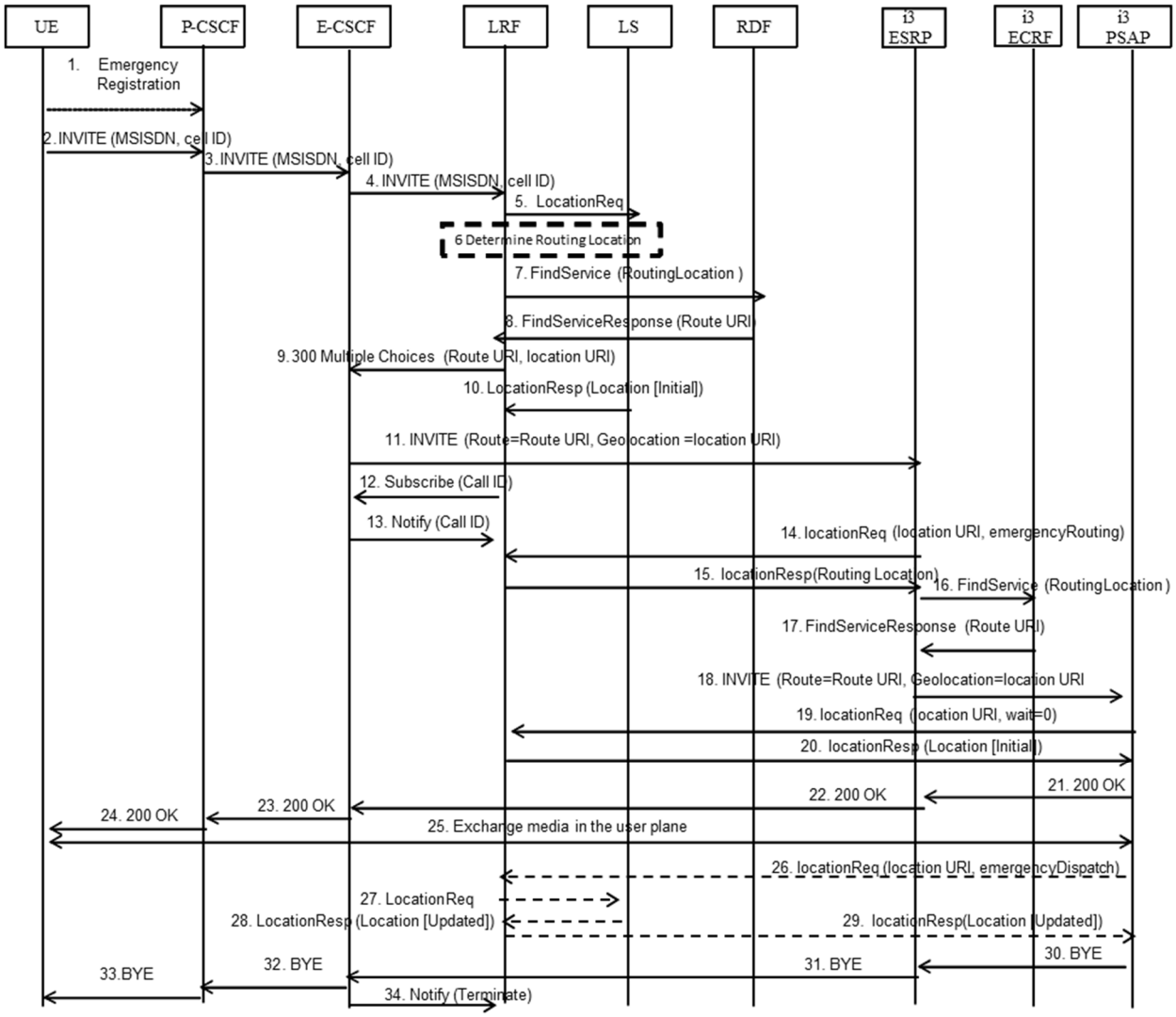

Figure 8.3 – Cell-Routed Call Delivery to NENA i3 ESInet – Location-by-Reference

Step 1. (Conditional) Emergency registration (if not already emergency registered and has credentials).

Step 2. The UE sends a SIP INVITE to P-CSCF.

Step 3. The P-CSCF, detecting an emergency call, forwards the SIP INVITE to the E-CSCF.

Step 4. The E-CSCF queries the LRF for location and/or route, by forwarding the SIP INVITE.

Step 5. The LRF interacts with the LS to acquire initial location (for presentation to the PSAP)/initiate position determination process.

Step 6. The LRF maps the cell ID received in the SIP INVITE message to a routing location that is the Associated Location designated for the appropriate PSAP for that cell. Note that Steps 5 and 6 may be performed in parallel, depending on the implementation.

Step 7. The LRF queries the RDF with the Routing Location (Associated Location) for routing information.

Step 8. The RDF responds by providing a Route URI.

Step 9. The LRF replies to the E-CSCF with location information (Reference Identifier consisting of a location URI, in this example) and the Route URI that will direct the call toward the ESInet.

Step 10. The LS responds with the initial location. This step may happen any time after Step 5 and before Step 20.

Step 11. The E-CSCF forwards the SIP INVITE (with any location information received from the LRF; in this example, a location URI) to the ESRP via an IBCF.

Step 12. The LRF sends a SIP SUBSCRIBE to the E-CSCF to be informed of the call state. (Alternatively, the Subscription may be done at the system start up and be applicable to all calls [not shown]).

Step 13. The E-CSCF sends an initial state NOTIFY to the LRF.

Step 14. In this example, the SIP INVITE contains a location URI, so the ESRP queries the LRF (as identified in the location URI) for Routing Location (Associated Location). This call flow illustrates the use of HELD as a de-reference protocol. The value of the responseTime parameter in the HELD locationRequest message will allow the LRF to determine whether an interaction with the LS should be initiated. Since the ESRP is requesting the Routing Location obtained in Step 6 (i.e., responseTime = “emergencyRouting”), the LRF does not initiate an interaction with the LS at this point in the call flow.

Step 15. The LRF supplies Routing Location (Associated Location) to the ESRP.

Step 16. (Informative) The ESRP queries the ECRF for routing information using LoST.

Step 17. (Informative) The ECRF replies to the ESRP with a Route URI (i.e., PSAP URI).

Step 18. The ESRP forwards the SIP INVITE to the PSAP.

Step 19. In this example, the SIP INVITE contains a location URI, so the PSAP queries the LRF (as identified in the location URI) for initial location (i.e., responseTime contains a wait timer value of “0”).

Step 20. The LRF supplies the initial location information from Step 10 to the PSAP. The initial location information is displayed at the PSAP CPE.

Step 21. The PSAP sends a SIP 200 OK to the ESRP. This Step may occur before Step 19.

Step 22. The ESRP forwards a SIP 200 OK to the E-CSCF via the BCF/IBCF.

Step 23. The E-CSCF forwards a SIP 200 OK to the P-CSCF.

NOTE: The E-CSCF sends a NOTIFY to the LRF based on Step 12 (not shown).

Step 24. The P-CSCF forwards a SIP 200 OK to the UE.

Step 25. Media is exchange in the user plane.

Step 26. (Optional) The PSAP queries the LRF (as identified in the location URI) for updated location information (responseTime parameter=“emergencyDispatch” in this example).

Step 27. (Conditional on Step 26) The LRF queries the LS for updated location. (Note that the value of the responseTime parameter [emergencyDispatch or a specific time value] will be used by the LRF to determine whether to query the LS.)

Step 28. (Conditional on Step 27) The LS returns updated location information to the LRF.

Step 29. (Conditional on Step 26) The LRF supplies updated location to the PSAP for display at the PSAP.

Step 30. The PSAP sends a SIP BYE to the ESRP. Note that this may be sent by the UE as well.

Step 31. The ESRP forwards a SIP BYE to the E-CSCF through the BCF/IBCF.

Step 32. The E-CSCF forwards a SIP BYE to the P-CSCF.

Step 33. The P-CSCF forwards a SIP BYE to the UE.

Step 34. The E-CSCF sends a termination SIP NOTIFY to the LRF in order to release resources. This may occur any time after Step 31.

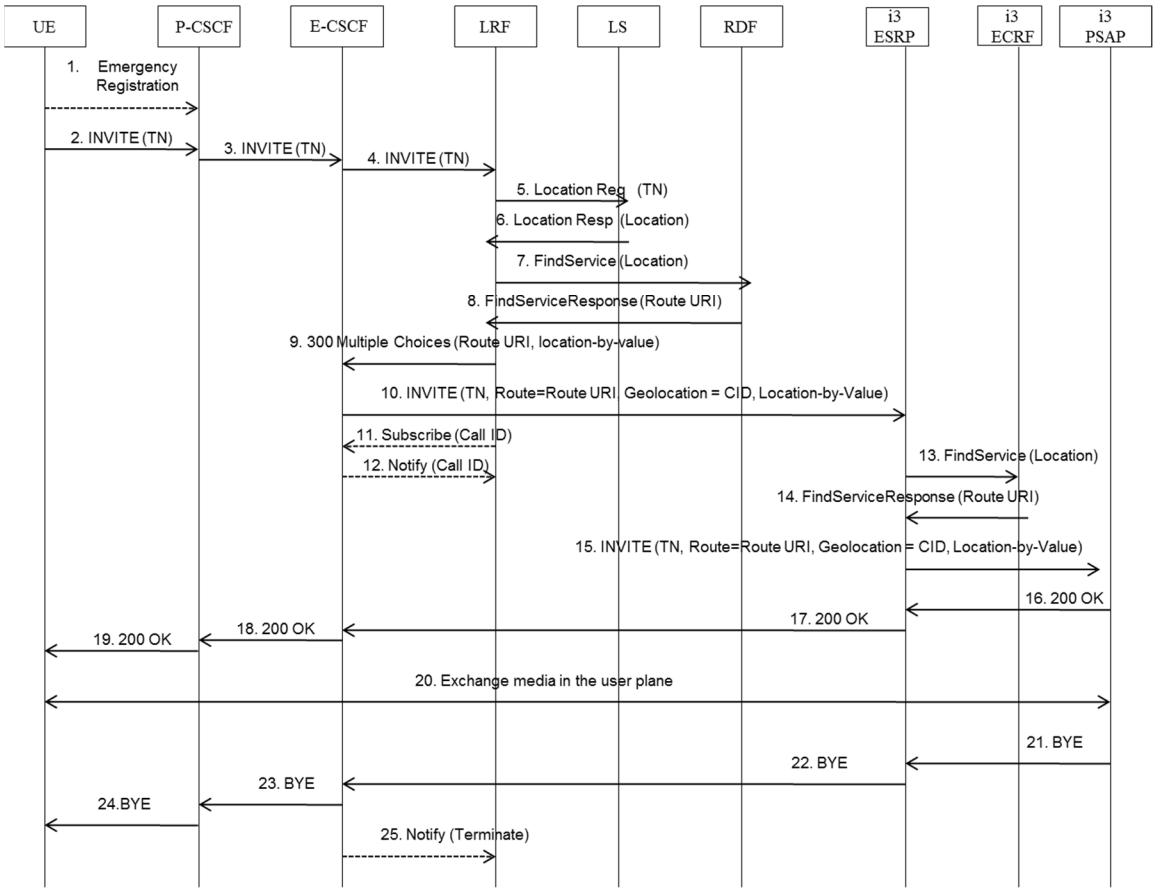

Figure 8.4 – Call Delivery to NENA i3 ESInet – Location-by-Value Delivered to ESInet

Step 1. (Optional) Emergency registration occurs (if not already emergency registered and has credentials).

Step 2. The UE sends a SIP INVITE to the P-CSCF. The emergency call origination is from a fixed UE and the SIP INVITE contains the user's telephone (i.e., E.164) number and no location information.

Step 3. The P-CSCF, detecting an emergency call, forwards the SIP INVITE to the E-CSCF.

Step 4. The E-CSCF queries the LRF for location and/or route, by forwarding the SIP INVITE.

Step 5. The LRF interacts with the LS to obtain the location of the Fixed UE, providing the user's telephone number to the LS.

Step 6. The LS maps the telephone number to a location value and responds with location value.

Step 7. The LRF queries the RDF for routing information using the location value obtained from the LS.

Step 8. The RDF responds by providing a Route URI.

Step 9. The LRF replies to the E-CSCF with location information (location-by-value, in this example) and a Route URI that will direct the call toward the ESInet.

Step 10. The E-CSCF forwards the SIP INVITE (with the location-by-value received from the LRF) to the ESRP via an IBCF/BCF.

Step 11. (Optional) The LRF sends a SIP SUBSCRIBE to the E-CSCF to be informed of the call state.

Step 12. (Conditional on Step 11) The E-CSCF sends an initial state NOTIFY to the LRF.

Step 13. (Informative) Within the ESInet, the ESRP queries the ECRF for routing information using the LoST protocol. The location-by-value and the emergency service URN are included in the LoST findService query.

Step 14. (Informative) The ECRF replies to ESRP with a PSAP URI.

Step 15. The ESRP forwards the SIP INVITE to the PSAP with location by value.

Step 16. The PSAP indicates that the call has been answered by returning a SIP 200 OK to the ESRP.

Step 17. The ESRP forwards the SIP 200 OK to the E-CSCF via the BCF/IBCF.

Step 18. The E-CSCF forwards the SIP 200 OK to the P-CSCF.

NOTE: E-CSCF may send a NOTIFY to LRF conditional on Step 11.

Step 19. The P-CSCF forwards the SIP 200 OK to the UE.

Step 20. Media is exchanged in the user plane.

Step 21. The PSAP sends a SIP BYE to the ESRP. Note that this may be sent by the UE as well.

Step 22. The ESRP forwards a SIP BYE to the E-CSCF through a BCF/IBCF.

Step 23. The E-CSCF forwards a SIP BYE to the P-CSCF.

Step 24. The P-CSCF forwards a SIP BYE to the UE.

Step 25. (Conditional on Step11) The E-CSCF sends a termination SIP NOTIFY to the LRF in order to release resources. This may occur any time after Step 22.

Figure 8.5 depicts a call flow where SHAKEN caller identity authentication and RPH signing is performed on an emergency call that is processed by an IMS originating network. Location-based routing performed by the originating network determines that the emergency call is to be routed via an i3 ESInet. This call flow assumes that the P-CSCF inserts a “verstat” parameter in the P-Asserted-Identity header, and Attestation-Info and Origination-Id header fields in the SIP INVITE message. The P-CSCF also populates an RPH in the SIP INVITE message. The exit IBCF in the IMS originating network interacts with the STI-AS to request signing of the caller identity and the RPH. Upon receiving a response from the STI-AS with identityHeader parameters associated with the signed caller identity and RPH, the exit IBCF creates and populates Identity headers in the outgoing SIP INVITE message and forwards the SIP INVITE message via a BCF to an ESRP in an i3 ESInet. The ESRP interacts with an STI-VS to request verification of the received Identity headers by forwarding the STI-VS the received SIP INVITE message. The STI-VS includes the verification results in the SIP INVITE message that it returns to the ESRP. Call processing continues according to the procedures specified elsewhere in this document, with the ESRP interacting with an ECRF to determine the routing for the emergency call. The ESRP forwards the SIP INVITE message with the caller identity (callback number) and associated verification results in the P-Asserted-Identity header, the attestation information conveyed in the associated Identity header, an Identity header containing the signed RPH, and associated verification results in the Priority-Verstat header field.

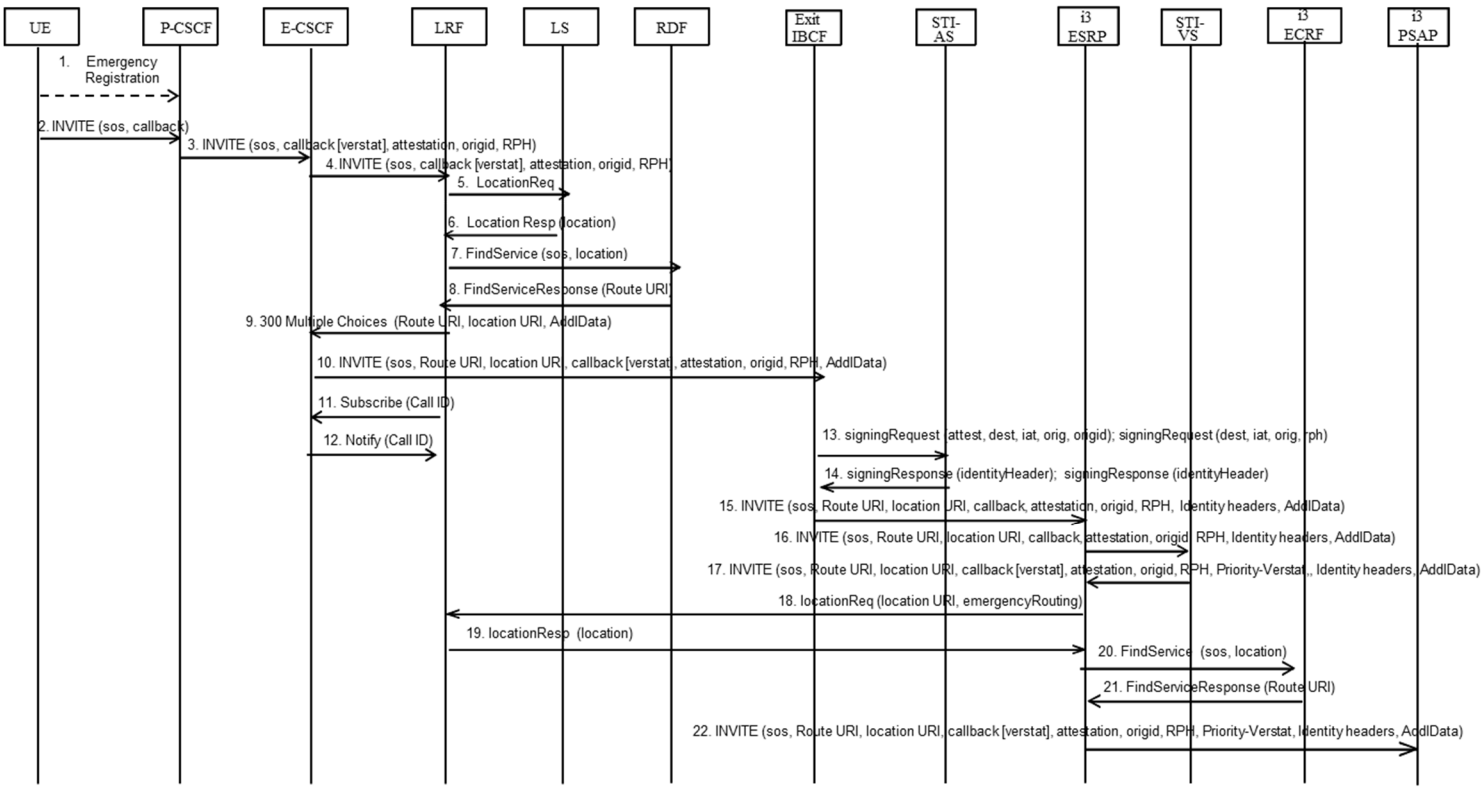

Figure 8.5 - Call Delivery to NENA i3 ESInet - Caller Identity and RPH Signing/Verification

Step 1. (Conditional) Emergency registration occurs (if not already emergency registered and has credentials).

Step 2. The originating SIP UE, which is authenticated to the P-CSCF, creates a SIP INVITE with a callback number (i.e., a telephone number identity) and an sos service URN in the Request URI.

Step 3. The P-CSCF in the originating network adds a P-Asserted-Identity header field asserting the callback number/caller identity of the originating SIP UE and an RPH with value “esnet.1”. This call flow assumes that, supported by local policy, the P-CSCF also inserts a “verstat” parameter in the P-Asserted-Identity header, and Attestation-Info and Origination-Id header fields in the SIP INVITE message for use by downstream calling identity authentication and verification processes. The P-CSCF passes the SIP INVITE to the E-CSCF.

Step 4. The E-CSCF passes the SIP INVITE message to the LRF to obtain location and routing information for the emergency call.

Step 5. The LRF selects a technique for acquiring location information based upon the call type. The LRF interacts with an LS to acquire location/initiate position determination, as applicable.

Step 6. The LS responds with location information.

Step 7. The LRF queries the RDF using location information and an sos service URN.

Step 8. The RDF returns a Route URI. In this example, the Route URI is associated with an ESRP in an i3 ESInet.

Step 9. The LRF redirects the callback to the E-CSCF by returning a 300 Multiple Choices message that contains a location information URI, a Route URI that directs the call toward the i3 ESInet, and Additional Data.

Step 10. The E-CSCF generates an outgoing SIP INVITE message, using the information received from the LRF as well as information received in the initial SIP INVITE message, and forwards it to the exit IBCF. In this example the SIP INVITE includes the sos service URN, a Route URI, a location URI, the callback number with associated “verstat” information, an Attestation-Info header, an Origination-Id header, the RPH, and Additional Data.

Step 11. The LRF sends a SIP SUBSCRIBE to the E-CSCF to be informed of call state. (Alternatively, the Subscription may be done at the system start-up and be applicable to all calls [not shown].)

Step 12. The E-CSCF sends an initial state NOTIFY to the LRF.

Step 13. The exit IBCF sends an HTTP POST containing two signing requests over the Ms reference point to the STI-AS. The signingRequest associated with the caller identity includes an "attest" parameter that contains the attestation information received by the IBCF in the Attestation-Info header field within the SIP INVITE, as well as other PASSporT information (i.e., "orig", and "dest" claims as well as the iat and origid). The second signingRequest includes the "rph" claim, along with "dest", "iat", and "orig" claims, as described in Clause 8.1.2. This call flow assumes that the exit IBCF populates an "auth" key with an assertion value of "esnet.1" in the "rph" claim based on receipt of the RPH.

Step 14. The STI-AS first determines through service provider-specific means the legitimacy of the telephone number identity and RPH populated in the INVITE. The STI-AS securely requests its private key from the SKS, and the SKS provides the private key in response (not shown). The STI-AS then returns an HTTP 200 OK message that includes a signingResponse that contains the signed identityHeader parameter associated with the caller identity and a signingResponse that contains the signed identityHeader associated with the RPH.

Step 15. The exit IBCF uses the information returned in the identityHeader parameters of the HTTP response to populate SIP Identity headers associated with the caller identity (callback number) and the RPH in the SIP INVITE message. The IBCF also removes the "verstat" prior to sending the call to the i3 ESInet. The exit IBCF then routes the SIP INVITE over the NNI via the ingress BCF to the ESRP in the ESInet using standard inter-domain routing resolution.

Step 16. The ESRP in the i3 ESInet forwards the received SIP INVITE message to the STI-VS.

Step 17. The STI-VS determines the STI-CR Uniform Resource Identifier (URI) and makes an HTTPS request to the STI-CR (not shown). The STI-VS validates the certificate and then extracts the public key. It uses the public key to verify the signature in the Identity header fields, which validate the caller identity and RPH content signed by the originating network STI-AS. The STI-VS may interact with the CVT based on local policy and agreements between the 9-1-1 Authority and the analytics/CVT provider (not shown). The STI-VS returns the SIP INVITE message to the ESRP. The SIP INVITE message includes a "verstat" tel uri parameter in the P-Asserted-Identity header and a Priority-Verstat header field indicating the result of the verification process. Depending on the results of the verification process, the "verstat" associated with the signed caller identity will be populated in the P-Asserted Identity header with a value set to "TN-Validation-Passed", "TN-Validation-Failed", or "No-TN-Validation". The Priority-Verstat header field associated with the signed RPH will be set to "RPH-Validation-Passed", "RPH-Validation-Failed", or "No-RPH-Validation".

Step 18. Since, in this example, the SIP INVITE contains a location URI, the ESRP queries the LRF (as identified in the location URI) for routing location (Associated Location). This call flow illustrates the use of HELD as a de-reference protocol. The value of the responseTime parameter in the HELD locationRequest message is set to "emergencyRouting".

Step 19. The LRF supplies routing location (Associated Location) to the ESRP.

Step 20. (Informative) The ESRP queries the ECRF for routing information using LoST.

Step 21. (Informative) The ECRF replies to the ESRP with a Route URI (i.e., PSAP URI).

Step 22. The ESRP passes the SIP INVITE message to i3 PSAP. In this example the SIP INVITE includes the sos service URN, a Route URI (associated with the i3 PSAP), a location URI, the callback number with associated "verstat" information, an Attestation-Info header, an Origination-Id header, the RPH, a Priority-Verstat header field, the Identity headers, and Additional Data.

8.2.2 Call Delivery to a Legacy Selective Router

Figure 8.6 illustrates legacy Selective Router termination for a call originated by a mobile device where cell-based location and MSISDN is provided in the initial SIP INVITE message. An Associated Location is used in some

wireless routing scenarios where the cell address or cell centroid cannot be used to route a call to the Selective Router. The Associated Location (shown as the Routing Location in the figure below) will be selected by the LRF and used by the RDF to determine routing. Unlike the NENA i3 ESInet, the legacy emergency services network cannot accept location in the call request and must query for location information once the call is delivered to the PSAP. This flow assumes that the regional ALI does not contain location information associated with the Common IMS Network user and the legacy emergency services network must query the LRF. In order to do this, a method such as wireless Non-Call-Associated Signaling (NCAS) or Wireline Compatibility Mode (WCM), as defined in ANSI J-STD-036-C-2 [Ref 7], is used.

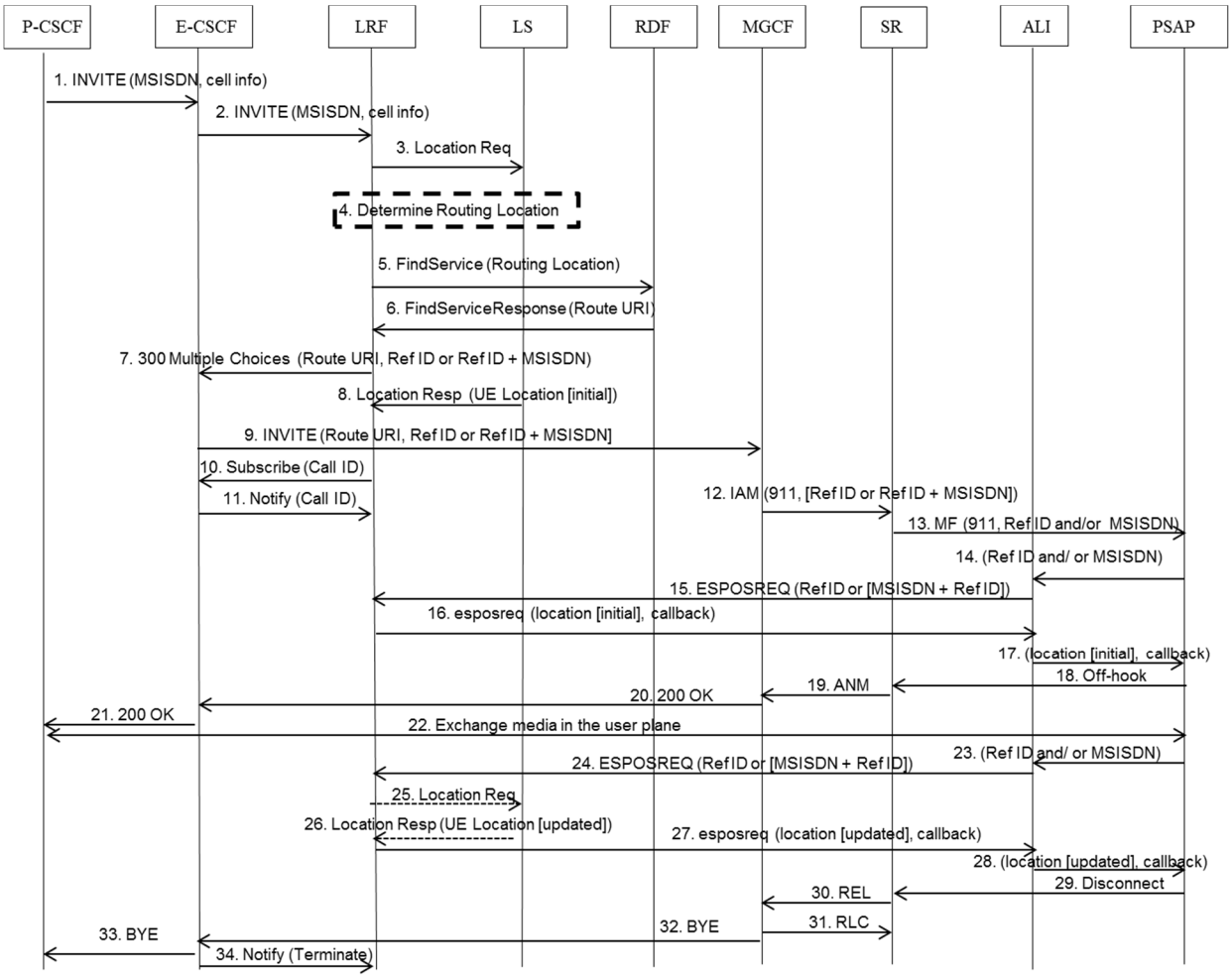

Figure 8.6 – Mobile Call Origination and Delivery to a Legacy Emergency Services Network using Associated Location

Step 1. The emergency call is initiated and the P-CSCF forwards it to the E-CSCF. This is an emergency call origination by a mobile device where MSISDN and cell-based location information is provided with the call.

Step 2. The E-CSCF forwards the SIP INVITE to the LRF.

Step 3. The LRF may select a location acquisition technique based upon the access type if this can be determined (e.g., using provided network access information). Since the emergency session request came from a mobile UE and it is to be routed based on cell-based location information, the LRF will initiate a query to the LS to acquire the UE's initial location (for presentation to the PSAP)/initiate the position determination process, but does not wait for a response before proceeding with call processing.

Step 4. The LRF determines the routing location (e.g., Associated Location) for the call based on the cell-based location information provided in the SIP INVITE (i.e., the LRF will map the cell ID received in the SIP INVITE to a routing location that is associated with the PSAP that, based

on pre-existing agreements, is supposed to receive the call). Note that Steps 3 and 4 may be performed in parallel, depending on the implementation.

Step 5. The LRF queries the RDF with the routing location (e.g., Associated Location) to obtain routing information for the call.

Step 6. The RDF returns a Route URI. In this example, the Route URI is associated with a route to a Selective Router in a legacy emergency services network.

Step 7. Based on the Route URI returned by the RDF, the LRF must select a Reference Identifier (i.e., ESRK or ESRD for a mobile origination) which the legacy emergency services network uses to route the call and to obtain location. An ESRK determines the destination and associated LRF and temporarily identifies the UE for the duration of the IMS emergency call. An ESRD just determines the destination and LRF. The LRF redirects the callback to the E-CSCF, passing the Reference Identifier (ESRK), or the Reference Identifier (ESRD or ESRK) and the callback number (MSISDN). (See Clause 8.5.2.1 for a description of how this information is populated in the 300 Multiple Choices message.)

Step 8. The initial location may be returned by the LS at any time after Step 3, and is cached in the LRF.

Step 9. The E-CSCF formats the SIP INVITE with the information received from the LRF and forwards the request to the MGCF containing the callback number and/or the Reference Identifier.

Step 10. The LRF subscribes to the state of the call. (Alternatively, the Subscription may be done at the system start up and be applicable to all calls [not shown]).

Step 11. The E-CSCF sends an initial state SIP NOTIFY to the LRF.

Step 12. The MGCF creates an SS7 IAM with either: (i) 9-1-1 in the Called Party Number parameter and the Reference Identifier in the Calling Party Number parameter; or (ii) 9-1-1 in the Called Party Number parameter, MSISDN in the Calling Party Number parameter, and the Reference Identifier in the Generic Digits Parameter, as described in Appendix D of ANSI J-STD-036-C-2 [Ref 7]. (See Clause 8.5.5 for further details related to SIP/ISUP SS7 mappings at the MGCF.)

Step 13. The Selective Router uses the Reference Identifier to determine the PSAP and delivers the call with the Reference Identifier and/or MSISDN. The call taker is alerted to the incoming call (not shown).

Step 14. The PSAP queries the ALI with the Reference Identifier and/or the MSISDN.

Step 15. The ALI sends a location request to the LRF that contains: (i) the Reference Identifier; or (ii) MSISDN and Reference Identifier. The location request also includes an indicator specifying that "initial" location is being requested[9].

Step 16. The LRF returns the callback number (MSISDN) and initial location information to the ALI.

Step 17. The ALI returns the callback number (MSISDN) and initial location information to the PSAP.

Step 18. When the PSAP answers the call, it returns an off-hook signal to the SR. Note that this may occur before Step 14.

Step 19. Upon receiving the off-hook signal, the SR generates an SS7 Answer Message (ANM) and sends it to the MGCF.

Step 20. Upon receiving the SS7 ANM, the MGCF sends a SIP 200 OK to the E-CSCF.

Step 21. The E-CSCF returns the SIP 200 OK to the P-CSCF. The P-CSCF passes the SIP 200 OK to the UE (not shown).

NOTE: The E-CSCF sends a NOTIFY to the LRF based on Step 10 (not shown).

Step 22. At this point, a two-way connection is established between the user and the PSAP.

Step 23. (Optional) The PSAP queries the ALI with the Reference Identifier and/or the MSISDN for updated/last known location.

---

[9] In the case where ALI receives only MSISDN from the PSAP, ALI retrieves the Reference Identifier from its internal database updated by the SR.

Step 24. (Conditional on Step 23) The ALI sends a location request to the LRF that contains: (i) the Reference Identifier; or (ii) MSISDN and Reference Identifier. The location request also includes an indicator specifying that either “updated” or “updated/last known” location is being requested.

Step 25. (Conditional on Step 24) The LRF interacts with the LS for the updated location information.

Step 26. (Conditional on Step 24) The LS returns updated location to the LRF.

Step 27. (Conditional on Step 23) The LRF returns the callback number and updated/last known location information to the ALI.

Step 28. The ALI returns the callback number (MSISDN) and updated/last known location information to the PSAP.

Step 29. At some point, the call is terminated. In this call flow, the PSAP terminates the call and a disconnect indication is sent to the SR.

Step 30. Upon receiving the disconnect signal, the SR generates an SS7 Release (REL) message and sends it to the MGCF.

Step 31. Upon receiving the SS7 REL message, the MGCF returns an SS7 Release Complete (RLC) message to the SR.

Step 32. The MGCF sends a SIP BYE to the E-CSCF.

Step 33. The E-CSCF forwards the SIP BYE to the P-CSCF (and then on to the UE).

Step 34. The E-CSCF sends termination SIP NOTIFY to the LRF in order to release resources.

8.2.3 Emergency Access Network Flows

Some of the access network types for which the procedures and requirements in this document are applicable with specific reference to IMS interaction, handover, and support of location are discussed in Annex F.

8.2.4 IMS Emergency Registration Flows

This clause describes support for IMS registration specific to support of emergency services, as shown in Figure 8-6.

IMS Emergency registration is always required for access types that include support for emergency bearers whenever the UE has sufficient credentials and either:

- Recognizes that the user has requested an emergency call; or
- Does not recognize the emergency call but receives a SIP 380 Redirect response from the network indicating an emergency call.

The access types for which this applies comprise LTE, HSPA, and eHRPD. The option allowed in 3GPP TS 24.229 [Ref 2] of establishing an IMS emergency call using a normal bearer and non-emergency IMS registration is not supported in North America for these access types, unless the emergency call is not recognized by the UE and is allowed to continue by a P-CSCF in the serving network. IMS emergency registration is also required for eHRPD access when roaming if the UE has sufficient credentials, and by all access types for a UE that has sufficient credentials but has not yet registered when an emergency call request is detected.

Prior to performing an IMS emergency registration, a UE shall obtain an emergency bearer if the access type is LTE, HSPA, or eHRPD.

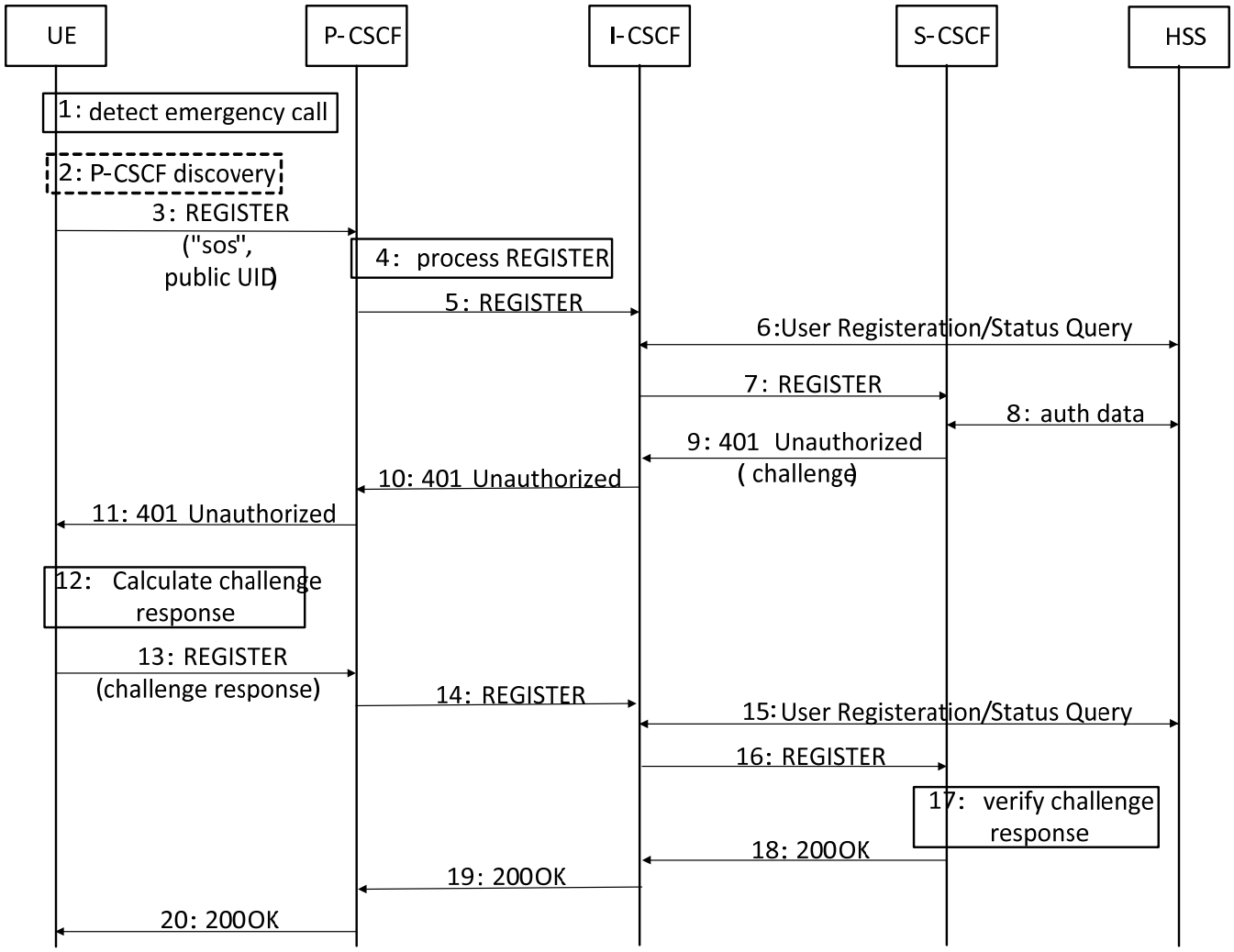

Figure 8.7 – IMS Emergency Registration

Step 1. Per 3GPP TS 23.167 [Ref 1], Clause 7.2.1, if the UE detects that the user is placing an emergency call, the UE attempts an emergency registration depending on the access type as described previously. If the UE is aware that it lacks sufficient credentials for an emergency registration (e.g., USIM-less), it does not attempt one, but instead skips ahead to attempt an emergency session establishment without registration.

- Per 3GPP TS 24.229 [Ref 2], Clause 5.1.6.2, the emergency registration includes an "sos" parameter in the SIP URI in the Contact header field, and uses the first provisioned public user identity (or a default or derived public user identity) in the From and To header fields.
- Per 3GPP TS 24.229 [Ref 2], Clause 5.1.1.2, the UE determines a public user identity, the private user identity, and the domain name for the Request-URI.

The REGISTER also includes (only a few of the more important fields are listed below):

- Both From and To header fields set to the SIP URI that contains the public user identity.
- A Contact header field set to include SIP URI(s) containing the IP address or FQDN of the UE in the hostport parameter.
- Optionally, a "+sip.instance" header field parameter containing the instance ID if the UE supports GRUU, multiple registrations, and has an IMEI or MEID available.
- A Via header field which includes the sent-by field containing the IP address or FQDN of the UE (and for UDP the port number for the response).
- A Request-URI set to the SIP URI of the domain name of the home network used to address the REGISTER request.

- Per 3GPP TS 23.167 [Ref 1], Clause 7.2.1, the implicit registration set of the SIP URI used in the emergency registration request contains an associated TEL-URI that is used to perform a callback to the user from the PSTN.

Step 2. The UE performs a P-CSCF discovery procedure, as specified in 3GPP 23.228 [Ref 34], in order to identify the target P-CSCF in the serving network for the emergency registration and emergency session establishment. This is normally done at the time the UE associates with the IP connectivity access network (IP-CAN), before attempting an emergency registration.

Step 3. The UE sends the SIP REGISTER request to the P-CSCF.

Step 4. Per 3GPP TS 24.229 [Ref 2], Clause 5.2.2, the P-CSCF (among other actions):

- Inserts a Route header field containing the URI of the next hop element:
    - If the P-CSCF is in the visited network, the next hop element is either a selected exit point in the visited network (e.g., an IBCF) or a selected entry point in the home network (e.g., IBCF or I-CSCF), per local policy. Depending on local policy, separate Route header fields may be added, one containing the exit point and the other containing the entry point. Or, the selected exit point may itself determine the entry point.
    - If the P-CSCF is in the home network, the next hop element is the either an I-CSCF or another element within the home network, per local policy.

In this particular example, the next hop element is I-CSCF.

Step 5. The P-CSCF sends the SIP REGISTER request to the home I-CSCF (based on the provided home domain name).

Step 6. The I-CSCF, upon receiving the SIP REGISTER message, interacts with the HSS to determine the status of the UE and determine the S-CSCF that has to be used for the emergency registration.

Step 7. The I-CSCF forwards the SIP REGISTER to the S-CSCF.

Step 8. The S-CSCF interacts with the HSS to obtain authentication data.

Step 9. The S-CSCF responds to the SIP REGISTER with a SIP 401 Unauthorized containing an authorization challenge.

Step 10. The I-CSCF forwards the SIP 401 Unauthorized response to the P-CSCF.

Step 11. The P-CSCF forwards the SIP 401 Unauthorized response to the UE.

Step 12. The UE calculates a challenge response.

Step 13. The UE sends another SIP REGISTER request containing the challenge response to the P-CSCF.

Step 14. The P-CSCF forwards the SIP REGISTER request to the I-CSCF.

Step 15. The I-CSCF, upon receiving the SIP REGISTER message, interacts with the HSS to determine the status of the UE and determine the S-CSCF that has to be used for the emergency registration.

Step 16. The I-CSCF forwards the SIP REGISTER to the S-CSCF.

Step 17. The S-CSCF verifies the challenge response.

- The S-CSCF will also register any other public identities included in the subscriber's provisioned implicit registration set (e.g., the UE may have omitted a Tel-URI from the SIP REGISTER request, but if the Tel-URI is within the implicit registration set which also contains the included SIP URI, that Tel-URI is also registered).

Step 18. The S-CSCF sends a SIP 200 OK response to the SIP REGISTER to the I-CSCF.

Step 19. The I-CSCF forwards the SIP 200 OK to the P-CSCF.

Step 20. The P-CSCF forwards the SIP 200 OK response to the UE.

8.2.5 IMS Emergency Session Origination Flows

This clause describes delivering emergency calls to two types of termination networks: a NENA i3 ESInet (designated using the “A” variant) and legacy emergency services network (designated using the “B” variant).

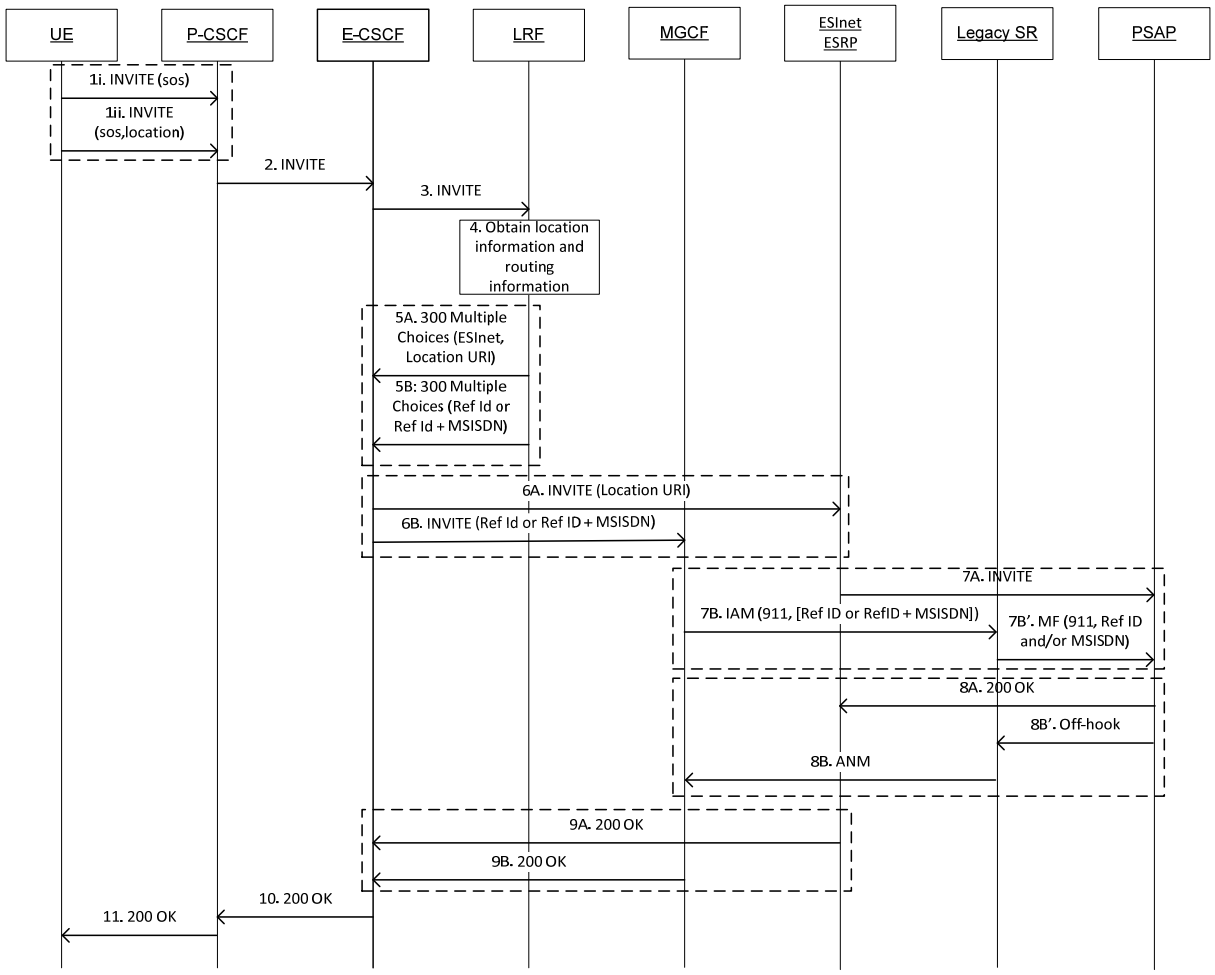

Figure 8.8 – Emergency Session Establishment

Step 1. The UE sends a SIP INVITE to the P-CSCF containing an emergency indication (e.g., in North America the user is expected to call 9-1-1 which results in the generic "urn:service:sos:" URN listed in the IANA registry[10]).

i. Either the UE does not include location if not available; or

ii. The UE includes its location if available (e.g., a UE connected via fixed access which received location via DHCP) by adding a PIDF-LO (see RFC 4119 [Ref 31], as modified by RFC 5491 [Ref 35] and RFC 5139 [Ref 36]) in the body of the SIP INVITE and a Geolocation header pointing to it.

Step 2. The P-CSCF, on detecting the emergency indication, forwards the SIP INVITE to the E-CSCF.

[10] Specifically, the IANA registry created by RFC 5031 [Ref 41]: the *'sos' Sub-Services* area of the *URN Service Labels* registry, located at < http://www.iana.org/assignments/urn-serviceid-labels/urn-serviceid-labels.txt >.

- If the SIP INVITE does not contain an emergency indication but the P-CSCF detects that it is an emergency session request (e.g., based on dialed number in the "tel:" URI), the P-CSCF may return a SIP 380 response to the UE containing an emergency indication. The UE handles the SIP 380 response as specified in 3GPP TS 24.229 [Ref 2] (e.g., reinitiate the emergency call or perform an emergency registration).
- Alternatively, the P-CSCF may continue the session origination and treat it as an emergency request by adding an emergency indication (i.e., an "sos:" URI determined from the dialed number or request URI) and forwarding it to the E-CSCF.
- Per 3GPP TS 23.167 [Ref 1], Clause 7.3, the P-CSCF checks whether the UE provided a TEL-URI as its identity in the SIP INVITE. If a TEL-URI is present, the P-CSCF checks its validity. If no TEL-URI is present and the P-CSCF is aware of a TEL-URI associated with the emergency registration, it adds the TEL-URI to the SIP INVITE.

Step 3. The E-CSCF forwards the request to the LRF to obtain location information and routing information[11].

- If no P-Asserted-Identity was provided, the E-CSCF inserts a P-Asserted-Identity header field set to a non-dialable callback number per J-STD-036-C-2 [Ref 7] if required for this type of call (e.g., LTE).
- If location (i.e., a PIDF-LO in the body with a Geolocation header pointing to it) was included by the UE (1ii), the E-CSCF includes it.

Step 4. The LRF may have the requested information cached, or may initiate position determination procedures (i.e., either SUPL or a control plane solution appropriate for the IP-CAN as described in Annex C). The LRF queries an RDF to determine the route towards the PSAP.

Step 5. The LRF redirects the call by returning a SIP 300 Multiple Choices response to the E-CSCF containing one or more emergency services URIs in a Contact header field.

Step 5A. The LRF inserts a Route URI associated with the NENA i3 ESInet in the Contact header field. When the LRF includes location information, it will be encoded as header fields of the URI in the Contact header field of the response. See Clause 8.5.2.1 for encoding location-by-reference and location-by-value.

Step 5B. The LRF inserts a Route URI associated with a legacy emergency services network in the form of a SIP URI with user=phone in the Contact header field. See Clause 8.5.2.1 for encoding of the Contact header field of the response, depending on the information required by the Selective Router.

Step 6. The E-CSCF updates the SIP INVITE with information returned by the LRF and forwards it per the Contact header URI set by the LRF.

Step 6A. The returned Contact header field URI is an ESInet ESRP.

- The E-CSCF copies the Contact header field of the SIP 300 Multiple Choices response to the Route header field of the outgoing SIP INVITE.
- The E-CSCF populates the outgoing SIP INVITE following the procedures described in Clauses 8.5.1 and 8.5.1.1.

Step 6B. The returned Contact header field contains a Route URI causing the call to be routed to a CS legacy Selective Router via an MGCF/MGW.

- The E-CSCF copies the Contact header field of the SIP 300 Multiple Choices response to the Request-URI and the BGCF URI is added to the topmost Route header field of the outgoing SIP INVITE.

[11] There may be cases in which the SIP INVITE contains location information sufficient to route the call which is sufficiently trusted or can be sufficiently verified that the LRF can use it directly, without first having to obtain location.

- The E-CSCF populates the other fields in the outgoing SIP INVITE following the procedures described in Clauses 8.5.1 and 8.5.1.1.

Step 7. The call request continues to the PSAP or legacy SR, as appropriate.

Step 7A. The ESInet ESRP queries an ECRF for routing information (not shown) and forwards the SIP INVITE to the PSAP. The location information provided to the PSAP in the forwarded SIP INVITE is unchanged from what was delivered to the ESInet ESRP in Step 8A.

Step 7B. The MGCF creates an SS7 IAM with either: (i) 9-1-1 as the Called Party Number parameter and the Reference Identifier as the Calling Party Number parameter; or (ii) 9-1-1 as the Called Party Number parameter, MSISDN as the Calling Party Number parameter, and the Reference Identifier in the Generic Digits Parameter, as described in Appendix D of ANSI J-STD-036-C-2 [Ref 7], and sends it to the legacy SR.

Step 7B. The legacy SR interacts with a Selective Routing Database to obtain routing information (not shown) and delivers the call request to the PSAP over a traditional or Enhanced MF interface.

Step 8. The PSAP is alerted (not shown) and the call is accepted by the PSAP.

Step 8A. The PSAP sends a SIP 200 OK response to the ESInet ESRP.

Step 8B'. The PSAP sends a call acceptance (i.e., off-hook) to the legacy SR.

Step 8B. The legacy SR generates an SS7 ANM in response to receiving the off-hook from the PSAP and sends it to the MGCF.

Step 9. The E-CSCF receives a SIP 200 OK response.

Step 9A. The ESInet ESRP sends a SIP 200 OK response to the E-CSCF.

Step 9B. The MGCF sends a SIP 200 OK response to the E-CSCF.

Step 10. The E-CSCF forwards the SIP 200 OK to the P-CSCF.

Step 11. The P-CSCF forwards the SIP 200 OK to the UE.

8.3 PSAP Callback Flows

A PSAP callback to a UE that previously originated an IMS emergency call may be routed by the PSAP via an i3 ESInet, and if so, the associated SIP INVITE message received by an IMS network may contain additional information that would not be present in an emergency callback that is routed by the PSAP via the PSTN. An IMS network must therefore be capable of receiving and processing a SIP INVITE message associated with an emergency callback that includes a Request-URI and a To header that contain the callback URI (i.e., the emergency caller's callback number from the P-Asserted-Identity or From header in the original emergency request), From and P-Asserted-Identity headers that contain a telephone number (TN) that is associated with the PSAP that is originating the callback, as well as a SIP Priority header set to "psap-callback", an RPH set to "esnet.0", and Identity headers that contain signed caller identity and RPH/Priority header information. Depending on the nature of the emergency, a SIP INVITE message associated with an emergency callback may include a SIP Privacy header.

As for emergency calls, the SHAKEN model specified in ATIS-1000074-E [Ref 45] can be used to authenticate and verify the caller identity information associated with an emergency callback. In addition, the SHAKEN model can be leveraged to cryptographically sign and verify the SIP RPH and Priority header fields in SIP INVITE messages associated with emergency callbacks using the PASSporT extension defined in IETF RFC 8443 [Ref 49] and the RPH assertion values and SIP Priority header claim described in IETF RFC 9027 [Ref 51], along with the associated STI protocols. The authentication/signing process for a callback call within an i3 ESInet will result in the creation of two Identity headers: one associated with the caller identity and one associated with the RPH/Priority header.

An IMS (home) network that receives a SIP INVITE associated with a callback call that contains a Priority header set to "psap-callback" may, based on local policy, apply special network handling of the call, such as bypassing services that might preclude the call from completing to the intended called party (i.e., the emergency caller), as described in IETF RFC 7090 [Ref 52]. A SIP INVITE associated with emergency callback that contains an RPH with

a value of “esnet.0” should be given priority treatment with regard to access to network resources over calls that do not contain an RPH value, in accordance with IETF RFC 7135 [Ref 53].

If an IMS network supports caller identity and RPH/Priority header verification, then upon receiving a SIP INVITE associated with an emergency callback that contains Identity headers, the IMS network should initiate an interaction with an STI-VS. Multiple architectures are possible to support the application of SHAKEN caller identity and RPH/Priority header verification procedures to emergency callbacks by an emergency caller’s home network. For emergency callbacks that are routed via an i3 ESInet/NGCS, an Outbound Call Interface Function (OCIF) in the i3 ESInet, if configured through operator policies, is responsible for invoking caller identity authentication and RPH/Priority header signing by passing the SIP INVITE message associated with the emergency callback to the Authentication Service (i.e., STI-AS). The OCIF will invoke the Authentication Service for emergency callbacks after call processing has completed, that is, after the target interconnected network has been determined to be an IP network. The OCIF will include the results of the authentication process (i.e., in the form of Identity headers) in the SIP INVITE message it passes to the interconnected IP network. When the emergency callback reaches the 9-1-1 caller’s home network, the Verification Service (i.e., the STI-VS) will be invoked. Depending on the architecture supported by the IMS network, the Verification Service may be invoked by an entry IBCF using an HTTP interface or by an IMS Call Session Control Function (e.g., S-CSCF) using a SIP interface. Call flows associated with these architectural alternatives are described below.

8.3.1 Emergency Callback with Verification Performed by Entry IBCF

Figure 8.9 illustrates a flow in which the entry IBCF in an IMS network interacts with an STI-VS to support verification of caller identity and RPH/Priority header information.

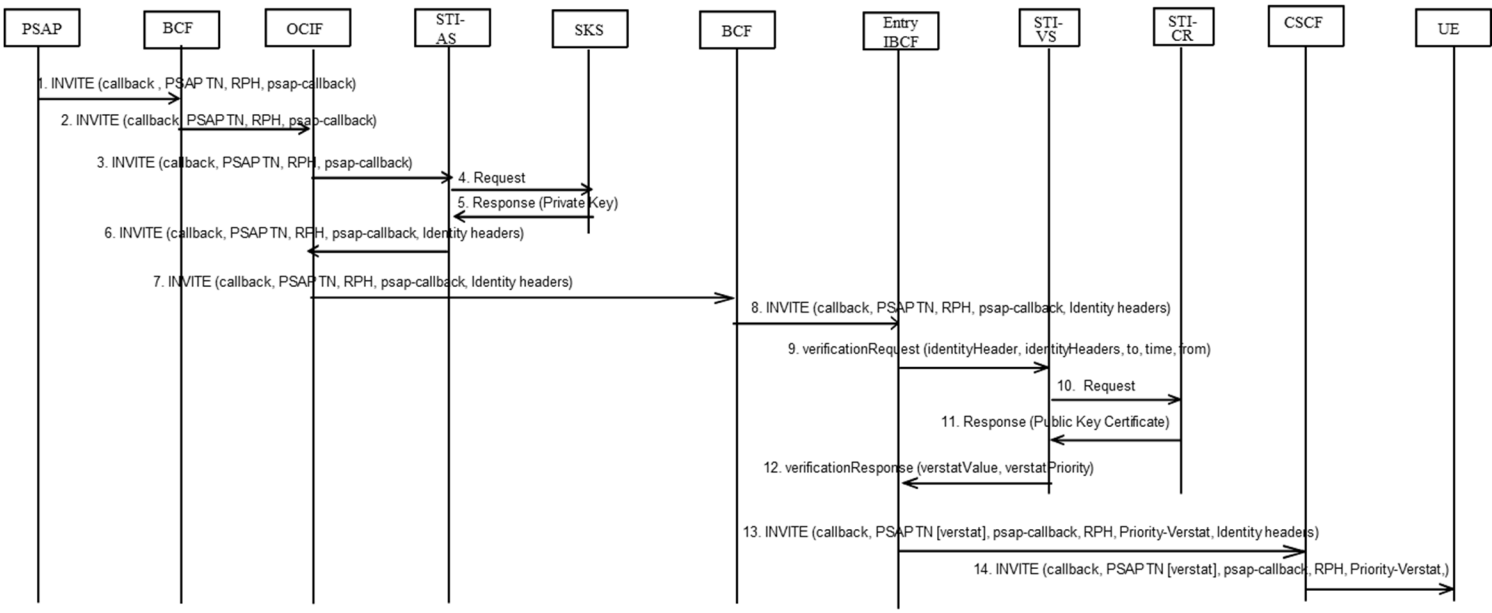

Figure 8.9 – Emergency Callback – Entry IBCF Interacts with STI-VS

Step 1. The PSAP Call Handling Function initiates a callback call with the callback URI from the original emergency call in the To header and Request-URI, the TN of the PSAP originating the callback (i.e., sip:TN@<psapdomain>;user=phone) in the From and P-Asserted-Identity headers, “psap-callback” in the Priority header, and “esnet.0” in the Resource-Priority header.

Step 2. The BCF forwards the INVITE to the OCIF (possibly via an ESRP [not shown]).

Step 3. The OCIF uses the destination address (i.e., the callback URI) in the Request-URI to determine the routing for the call. Before forwarding the call to an interconnecting IP network, the OCIF passes the SIP INVITE message to the STI-AS for authentication and signing of the caller identity and signing of the RPH and SIP Priority header.

Note: The STI-AS must be invoked after originating call processing

Step 4. The STI-AS in the NGCS provider network first determines through service provider-specific means the legitimacy of the telephone number identity and RPH and SIP Priority header

values being used in the INVITE. The STI-AS then securely requests its private key from the SKS.

Step 5. The SKS provides the private key in the response, and the STI-AS signs the caller identity and the RPH/SIP Priority header and adds an Identity header field per RFC 8224 [Ref 50] associated with the caller identity in the P-Asserted-Identity header field and an Identity header associated with the signed RPH/SIP Priority header.

Step 6. The STI-AS passes the INVITE back to the NGCS OCIF.

Step 7. If the BCF is not incorporated in the OCIF, it routes the call to the egress BCF.

Step 8. The INVITE is routed over the NNI through the standard inter-domain routing configuration to the entry IBCF in the emergency caller's home network.

Step 9. The entry IBCF initiates a verificationRequest in an HTTP POST message to the STI-VS that includes an identityHeader parameter associated with the caller identity, an identityHeaders parameter associated with the RPH/SIP Priority header, as well as a "to" parameter containing the destination identity from the To header, a "from" parameter containing the asserted identity from the From or P-Asserted-Identity, and a "time" parameter based on the Date header field in the incoming request.

Note: The STI-VS must be invoked before terminating call processing.

Step 10. The STI-VS uses the "x5u" field in the PASSporT Protected Header per RFC 8225 [Ref 48] to determine the STI-CR Uniform Resource Identifier (URI) and makes an HTTPS request to the STI-CR to obtain the public key certificates associated with the PASSporTs.

Step 11. The STI-CR returns the public key certificates that will be used by the STI-VS to validate the signatures in the PASSporTs.

Step 12. The STI-VS validates the certificates (see Clause 5.3.1 of ATIS-1000074-E [Ref 45] for details) and then extracts the public key. It constructs the RFC 8224 [Ref 50] format and uses the public key to verify the signatures in the identityHeader and identityHeaders parameters, which validates the caller identity and RPH/SIP Priority header field content used when the caller identity and RPH/SIP Priority header content were signed by the STI-AS. The STI-VS may interact with the CVT based on local policy and agreements between the emergency caller's home service provider and the CVT provider (not shown).

Depending on the result of the validation process, the STI-VS returns a verificationResponse to the IBCF in an HTTP 200 OK message containing a verstatValue parameter (associated with the "identityHeader" parameter in the verificationRequest) and a "verstatPriority" parameter (associated with the "rph" and "sph" claims in the "identityHeaders" parameter in the verificationRequest). Depending on the results of the verification process, the "verstatValue" associated with the signed caller identity will be set to "TN-Validation-Passed", "TN-Validation-Failed", or "No-TN-Validation", and the "verstatPriority" associated with the signed RPH/SIP Priority header will be set to "ECB-RPH-Validation-Passed", "ECB-RPH-Validation-Failed", or "No-ECB-RPH-Validation".

Note: Error cases where verification fails are discussed in Clause 5.3.2 of ATIS-1000074-E [Ref 45].

Step 13. The IBCF continues to set up the call to the CSCF. The SIP INVITE message includes the callback number associated with the emergency caller, the PSAP telephone number and associated verstat (populated based on the content of the verstatValue parameter returned in the verificationResponse), the RPH set to "esnet.0", a Priority header set to "psap-callback", a Priority-Verstat header field (populated based on the content of the verstatPriority parameter in the verificationResponse), and the Identity headers.

Step 14. The CSCF continues to set up the call to the UE associated with the emergency caller. Whether the Identity headers are passed to the called UE is a matter of local policy. This call flow example assumes that the Identity headers are not passed to the called UE.

Note: If a Privacy header is included in the SIP INVITE message associated with an emergency callback, no P-Asserted-Identity header will be passed to the called UE. The From header will consist of a sip URI of the form: "sip:anonymous@anonymous.invalid". It is proposed that the "verstat" resulting from applying the verification process to the PSAP TN in the P-Asserted-Identity header will be conveyed to the UE as a parameter in this sip URI. This is subject to verification by IETF.

8.3.2 Emergency Callback with Verification Performed by CSCF

Figure 8.10 illustrates a flow in which the CSCF in an IMS network interacts with an STI-VS to support verification of caller identity and RPH/Priority header information.

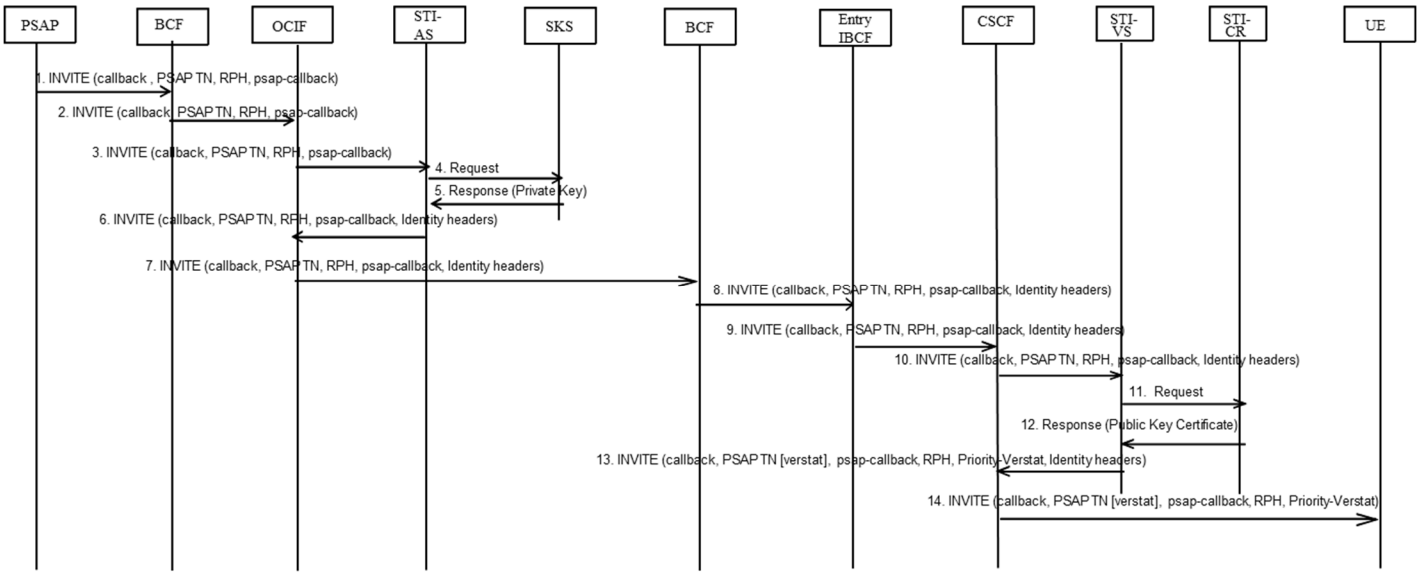

Figure 8.10 – Emergency Callback – CSCF Interacts with STI-VS

Step 1. The PSAP Call Handling Function initiates a callback call with the callback URI from the original emergency call in the To header and Request-URI, the TN of the PSAP originating the callback (i.e., sip:TN@<psapdomain>;user=phone) in the From and P-Asserted-Identity headers, "psap-callback" in the Priority header, and "esnet.0" in the Resource-Priority header.

Step 2. The BCF forwards the INVITE to the OCIF (possibly via an ESRP [not shown]).

Step 3. The OCIF uses the destination address (i.e., the callback URI) in the Request-URI to determine the routing for the call. Before forwarding the call to an interconnecting IP network, the OCIF passes the SIP INVITE message to the STI-AS for authentication and signing of the caller identity and signing of the RPH and SIP Priority header.

Note: The STI-AS must be invoked after originating call processing

Step 4. The STI-AS in the NGCS provider network first determines through service provider-specific means the legitimacy of the telephone number identity and RPH and SIP Priority header values being used in the INVITE. The STI-AS then securely requests its private key from the SKS.

Step 5. The SKS provides the private key in the response, and the STI-AS signs the caller identity and the RPH/SIP Priority header and adds an Identity header field per RFC 8224 [Ref 50] associated with the caller identity in the P-Asserted-Identity header field and an Identity header associated with the signed RPH/SIP Priority header.

Step 6. The STI-AS passes the INVITE back to the NGCS OCIF.

Step 7. If the BCF is not incorporated in the OCIF, it routes the call to the egress BCF.

Step 8. The INVITE is routed over the NNI through the standard inter-domain routing configuration to the entry IBCF in the emergency caller's home network.

Step 9. The entry IBCF forwards the SIP INVITE message to the CSCF.

Step 10. The CSCF forwards the SIP INVITE message to the STI-VS.

Note: The STI-VS must be invoked before terminating call processing.

Step 11. The STI-VS uses the "x5u" field in the PASSporT Protected Header per RFC 8225 [Ref 48] to determine the STI-CR Uniform Resource Identifier (URI) and makes an HTTPS request to the STI-CR to obtain the public key certificates associated with the PASSporTs.

Step 12. The STI-CR returns the public key certificates that will be used by the STI-VS to validate the signatures in the PASSporTs.

Step 13. The STI-VS validates the certificates (see Clause 5.3.1 of ATIS-1000074-E [Ref 45] for details) and then extracts the public key. It constructs the RFC 8224 [Ref 50] format and uses the public key to verify the signatures in the Identity header fields, which validates the caller identity and RPH/SIP Priority header field content used when the caller identity and RPH/SIP Priority header content were signed by the STI-AS. The STI-VS may interact with the CVT based on local policy and agreements between the emergency caller's home service provider and the CVT provider (not shown).

Depending on the result of the validation process, the STI-VS returns a SIP INVITE message to the CSCF that contains a "verstat" set to "TN-Validation-Passed", "TN-Validation-Failed", or "No-TN-Validation" as a URI parameter in the P-Asserted-Identity header, and verification status information associated with the RPH/SIP Priority header set to "ECB-RPH-Validation-Passed", "ECB-RPH-Validation-Failed", or "No-ECB-RPH-Validation" in a Priority-Verstat header field.

Note: Error cases where verification fails are discussed in Clause 5.3.2 of ATIS-1000074-E [Ref 45].

Step 14. The CSCF continues to set up the call to the UE associated with the emergency caller. Whether the Identity headers are passed to the called UE is a matter of local policy. This call flow example assumes that the Identity headers are not passed to the called UE.

Note: If a Privacy header is included in the SIP INVITE message associated with an emergency callback, no P-Asserted-Identity header will be passed to the called UE. The From header will consist of a sip URI of the form: "sip:anonymous@anonymous.invalid". It is proposed that the "verstat" resulting from applying the verification process to the PSAP TN in the P-Asserted-Identity header will be conveyed to the UE as a parameter in this sip URI. This is subject to verification by IETF.

8.4 Location Acquisition & Conveyance Flows

For LTE and HSPA access, Annex C provides an informative description of procedures that may be used to acquire and convey location to a NENA i3 PSAP or legacy PSAP. The procedures align with the 3GPP Control Plane solution defined in 3GPP TS 23.271 [Ref 5] and OMA user plane SUPL solution [Ref 11] with no deviations or exceptions.

8.5 Stage 3 Description

This clause defines stage 3 procedures for the originating network and UE. The description includes clarifications and specific use for North America. This clause references specific standards and illustrates the differences for North America. This clause also illustrates header usage and message examples. The examples in this clause are informative.

8.5.1 Procedures & Header Usage for the Emergency CSCF

For North America, the E-CSCF shall follow the procedures in Clauses 4 and 5.11.1 General of 3GPP TS 24.229 [Ref 2] with the following exception:

1. Based on the requirement E-CSCF-050, privacy does not apply.
2. Based on the requirement E-CSCF-020, the E-CSCF shall always query the LRF. An external server is out of scope of this standard.

For North America the E-CSCF shall follow the procedures in 3GPP TS 24.229 [Ref 2], Clause 5.11.3, *Use of LRF*, with the following clarifications.

By convention, the E-CSCF uses the format of the URI in the Contact header of the SIP 300 Multiple Choices response to determine if the call is to be routed to a PSAP served by a legacy emergency services network or a PSAP served by an ESInet. A Directory Number (DN), which can be represented by a SIP URI with user=phone

(e.g., sip: +17735554321@carrier.example.net;user=phone), returned in the Contact header denotes a PSAP served by a legacy emergency services network and a sip URI (e.g., sip:esrp.esinetprovider.net;lr) denotes a PSAP served by the ESInet. Note that the DN is used within the originating network and there are no restrictions in assigning this DN since it will not be used outside the originating network.

3GPP TS 24.229 [Ref 2], Clause 5.11.3, “a) at step 6” specifies the action for an emergency call towards a PSAP served by the ESInet and is denoted by a sip URI in the Contact header of the SIP 300 Multiple Choices response. For North America, if the E-CSCF receives an initial SIP INVITE message associated with an emergency call that includes a Replaces option tag in the Supported header, the E-CSCF shall remove the Replaces option tag from the Supported header before forwarding the SIP INVITE message toward the ESInet, as specified in requirement E-CSCF-080.

3GPP TS 24.229 [Ref 2], Clause 5.11.3, “b) at step 6” specifies the action for an emergency call towards a PSAP served by a legacy emergency services network and is denoted by the use of a DN (in the form of a sip URI with user=phone) in the Contact header of the SIP 300 Multiple Choices response.

If no P-Asserted-Identity (PAI) header field is present in a SIP INVITE message received from a P-CSCF, and the UE does not have sufficient credentials, the E-CSCF shall insert a non-dialable callback number, derived as described in E-CSCF-010, in the PAI header of the SIP INVITE message prior to sending the SIP INVITE to the LRF.

The E-CSCF shall also follow the procedures adopted in Clause 5.11.3, “e)”, of 3GPP TS 24.229 [Ref 2], based on the requirement E-CSCF-060.

If the E-CSCF receives a SIP 300 Multiple Choices message from an LRF that contains a Contact URI parameter of “Call-Info”, it shall create a Call-Info header containing the value provided in the SIP 300 Multiple Choices message and populate it in the outgoing SIP INVITE message. Additionally, if the received SIP INVITE message contains a Call-Info header, it shall be passed on unmodified.

If the E-CSCF receives a SIP 300 Multiple Choices message that contains a Contact URI parameter with hname “body” and Additional Call Data “by value”, it shall replace the entire message body of the outgoing SIP INVITE message with the value of the header field within the Contact URI with hname "body”.

As described in Clause 5.11.3 of 3GPP TS 24.229 [Ref 2], if the E-CSCF does not receive a SIP 300 Multiple Choices in response to a request sent to the LRF within an operator settable timeout, the E-CSCF shall use a default URI value (configured in the E-CSCF) in the outgoing SIP INVITE message.

8.5.1.1 Header Usage

This clause denotes specific use of headers in this standard in compliance with the respective RFCs. Only pertinent headers are discussed.

Call-Info Header

The “Call-Info” header parameter will be returned in the Contact header of a SIP 300 Multiple Choices message to support the delivery of Additional Call Data. It will either contain a Reference URI (Ref URI), or it will contain a content-ID (CID) that points to the location in the message body of the Additional Call Data “by-value”. If received in a SIP 300 Multiple Choices message, the E-CSCF will add the ‘call-info’ header to the outgoing SIP INVITE message.

Request URI

The Request URI received from the P-CSCF contains the emergency services URN (e.g., urn:service:sos). On an outgoing initial SIP INVITE toward an ESInet, the E-CSCF shall copy the emergency services URN received in the Request URI of the incoming SIP INVITE from the P-CSCF to the Request URI header of the outgoing SIP INVITE message.

Example:

```
INVITE urn:service:sos SIP/2.0
```

On an outgoing initial SIP INVITE towards a legacy emergency service network, the E-CSCF shall copy the content of the Contact header of the SIP 300 Multiple Choices response to the Request URI.

Example:

```
INVITE sip:+17735554321@carrier.example.net;user=phone SIP/2.0
```

From Header

The From header represents the calling UE if known.

Examples:

UE known and registered UE.

```
From:+13125551234<sip:+13125551234@carrier.example.net;user=phone>;tag=23ac
```

UE unknown or unregistered UE.

```
From:Anonymous<sip:Anonymous@Anonymous.invalid>;tag=23ac
```

Contact Header

The Contact header received from a P-CSCF represents the address of the UE.

Example:

```
Contact: <sip:+13125551234@ue.carrier.example.net;user=phone>
```

The Contact header received in a SIP 300 Multiple Choices message from an LRF contains the Route URI provided by the RDF, and may also contain other parameters. (See Annex E.4 and E.5 for examples.)

The E-CSCF shall pass the Contact header received in the SIP INVITE message from the P-CSCF in the outgoing SIP INVITE message sent toward the ESInet or legacy emergency services network.

P-Asserted-Identity

If the originating IMS network supports caller identity authentication, then based on local policy, the P-Asserted Identity (PAI) header field received by the E-CSCF from the P-CSCF in a SIP INVITE associated with an emergency call may contain a "verstat" as a URI parameter in the tel URI or SIP URI with a user=phone that represents the callback number.

If the call is destined for an ESInet, the PAI represents the callback number. If the call is destined for a legacy emergency services network, it represents the Reference Identifier or the callback number. The E-CSCF shall follow the procedures in Clause 5.11.3 of 3GPP TS 24.229 [Ref 2] for populating the PAI header in an outgoing SIP INVITE message sent toward the ESInet or legacy emergency services network.

Examples:

For an emergency call destined for a legacy emergency services network, the PAI returned by the LRF Contact header parameter in the SIP 300 Multiple Choices message and populated by the E-CSCF in the outgoing SIP INVITE message may contain either the Reference Identifier created by the LRF or the callback number.

```
P-Asserted-
Identity:<sip:+13125551234;cpc=emergency;oli=02@carrier.example.net;user=phone>
```

For an ESInet, the PAI contains the caller's callback number.

```
P-Asserted-Identity:<sip:+13125551234@carrier.example.net;user=phone>
```

For an emergency call routed via an ESInet from an originating network that supports caller identity authentication, the PAI may include a “verstat” parameter as indicated below.

```
P-Asserted-Identity:<sip:+13125551234;verstat=TN-Validation-Passed@carrier.example.
net;user=phone>
```

P-Charge-Info Header

If the P-Charge-Info header is received by the E-CSCF in the SIP INVITE message from the P-CSCF, or in the SIP 300 Multiple Choices message from the LRF, the E-CSCF will include the P-Charge-Info header in the outgoing SIP INVITE message. If the E-CSCF receives a P-Charge-Info field in a SIP 300 Multiple Choices message, the E-CSCF will replace any P-Charge-Info header received in the original request with this value.

Example:

```
P-Charge-Info: <sip: +17326996201;npi=001;noa=004@domain;user=phone>
```

P-Access-Network-Info Header

The P-Access-Network-Info header may be sent to the E-CSCF to identify cell sites and sectors or access points.

Example:

```
P-Access-Network-Info:3GPP-E-UTRAN-FDD;utran-cell-id-3gpp=0AE212345608A41F9
```

P-Charging-Vector Header

For use in this standard, the P-Charging-Vector header is used to pass the carrier identifier to the LRF and potentially to the ESInet and is populated in accordance with RFC 3455 [Ref 42].

Example:

```
P-Charging-Vector:icid=34c23c445902;icid-generated-
at=ecscf.carrier.example.net;orig-ioi=carrier.example.net
```

Geolocation Header

The Geolocation header may be received from the P-CSCF along with the location of the UE. It will point to the location of the UE contained within the PIDF-LO of the message body. The E-CSCF shall pass this header in the outgoing SIP INVITE to the LRF.

If a Geolocation header is received in a SIP INVITE from a P-CSCF, and the SIP 300 Multiple Choices returned by the LRF does not contain a header parameter in the Contact-URI header with parameter name “Geolocation”, the E-CSCF will pass the Geolocation header received in the SIP INVITE from the P-CSCF in the outgoing SIP INVITE.

If the SIP 300 Multiple Choices response contains a header parameter in the Contact-URI header with parameter name “Geolocation”, the E-CSCF will use the content of the “Geolocation” header parameter to create (or replace) a Geolocation header in the outgoing SIP INVITE.

If the call is being routed to a PSAP served by the ESInet, the “Geolocation” header parameter will either contain a location reference URI, or it will contain a content-ID (CID) that points to the location in the message body where the location value is. If the call is being routed to a PSAP served by a legacy emergency services network, the “Geolocation” header parameter will contain the Reference Identifier created by the LRF.

Example of location-by-reference:

```
Geolocation:<http:lrf.lrfprovider.net/9xkei90z>
```

Example of location-by-value:

```
Geolocation: <cid:target123@someoperator.example.com>
```

Example of a Geolocation header that contains a Reference Identifier:

```
Geolocation: <sip:2025111212@lrf.example.com>
```

Geolocation-Routing Header

If the E-CSCF receives a Geolocation-Routing header in an SIP INVITE from a P-CSCF, it will pass this header in the outgoing SIP INVITE it sends to the LRF.

If a Geolocation-Routing header is received in a SIP INVITE from a P-CSCF, and the SIP 300 Multiple Choices returned by the LRF does not contain a header parameter in the Contact-URI header with parameter name "Geolocation-Routing", the E-CSCF will pass the Geolocation-Routing header received in the SIP INVITE from the P-CSCF in the outgoing SIP INVITE.

If the SIP 300 Multiple Choices message returned by the LRF contains a header parameter in the Contact-URI header with parameter name "Geolocation-Routing", the E-CSCF will use the content of the "Geolocation-Routing" header parameter of the Contact-URI in the SIP 300 Multiple Choices response to create (or replace) a Geolocation-Routing header in the outgoing SIP INVITE. As described in Clause 8.5.2, if the call is being routed to a PSAP served by the ESInet, the "Geolocation-Routing" header parameter will contain the value “yes”. If the call is being routed to a PSAP served by a legacy emergency services network, the ‘geolocation-routing’ header parameter will contain the value “no”.

Examples:

```
Geolocation-Routing:yes
```

```
Geolocation-Routing:no
```

Content-Type

The Content-Type header field indicates the media type of the message-body sent to the recipient. For calls sent by the E-CSCF to a NENA i3 ESInet, where location-by-value and/or Additional Call Data “by-value” has been returned in the SIP 300 Multiple Choices message, the E-CSCF will populate a Content-Type value of “multipart/mixed” (as received in the 300 Multiple Choices message) in the outgoing SIP INVITE message. The E-CSCF must associate a Content-Type value of “application/sdp” with the portion of the body that carries the SDP information, a Content-Type value of “application/pidf+xml” with the portion of the body that carries the location-by-value (PIDF-LO), and a Content-Type value of “application/addDataProviderinfo+xml with the portion of the body that carries the Additional Call Data “by-value”.

```
Content-Type: multipart/mixed; boundary=boundary1
   Content-Length: ...

   --boundary1

   Content-Type: application/sdp

   v=0
   o=UserA 2890844526 2890844526 IN IP4 here.com
   s=Session SDP
   c=IN IP4 pc33.someoperator.com
   t=0 0
   m=audio 49172 RTP/AVP 0
   a=rtpmap:0 PCMU/8000

   --boundary1

   Content-Type: application/pidf+xml
   Content-ID: target123@someoperator.example.com
        .
        .
```

```
    .
--boundary1—
Content-Type: application/addDataProviderinfo+xml
     Content-ID: <1234567890@atlanta.example.com>

     ...Additional Data goes here

     --boundary1--
```

Route Header

The E-CSCF shall include Route header(s) in an outgoing SIP INVITE message associated with an emergency call. The E-CSCF shall populate the Route header(s) based on the procedures specified in Clause 5.11.3 of 3GPP TS 24.229 [Ref 2].

Origination-Id Header

If the originating IMS network supports caller identity authentication, a SIP INVITE received by the E-CSCF from the P-CSCF in a SIP INVITE associated with an emergency call may contain an Origination-Id header field, set to a UUID identifying the P-CSCF which is configured based on local policy. See subclause 7.2.19 of 3GPP TS 24.229 for further information. If received in the SIP INVITE from the P-CSCF, the E-CSCF shall pass the Originating-Id header field forward in the outgoing SIP INVITE message associated with an emergency call.

Attestation-Info Header

If the originating IMS network supports caller identity authentication, a SIP INVITE received by the E-CSCF from the P-CSCF in a SIP INVITE associated with an emergency call may, based on local policy, contain an Attestation-Info header field, set according to subclause 7.2.18 of 3GPP TS 24.229 [Ref 2]. If received in the SIP INVITE from the P-CSCF, the E-CSCF shall pass the Attestation-Info header field forward in the outgoing SIP INVITE message associated with an emergency call.

8.5.2 Procedures & Header Usage for the Location Retrieval Function

The LRF procedures are defined in 3GPP TS 24.229 [Ref 2], Clauses 4 and 5.12. For North America, the following considerations are applicable.

If the P-Access-Network-Information indicates the UE is a mobile access type defined in clause 9 and routing is based on cell, then the LRF shall determine a civic or geodetic location associated with the cell serving the UE to be used for routing.

If the LRF must obtain location (initial or updated) of the UE from an LS, then the LRF shall acquire location from the LS using a protocol specified in Clause 8.1.1 for the L0 reference point.

If the network supports mobile emergency calls with control plane location services that use MLP [Ref 8] as the protocol on the L0 reference point, the LRF shall support sending location requests, and receiving location responses and location reports per Annex B. When the location report (i.e., ELR) includes both the LS identity and the core network serving identity, then the identified LS serves the identified core network identity. When the LS identity is included in the location report, it identifies the LS that shall be invoked by the LRF for subsequent location requests. If the LS identity is not included in the location report (e.g., on handover when reported by the source LS), or when the core network identity is received in a location response (e.g., handover during positioning), then the LRF shall determine the LS associated with the reported core network identity for subsequent location requests, based on implementation-specific mechanisms (e.g., mapping core network identity to LS).

If the LRF uses control plane location services to support location continuity for mobile emergency calls, then the LRF shall be able to receive location reports from the LS containing the identity of the new core network entity serving the UE, using the MLP protocol specified in Clause 8.1.1 for the L0 reference point.

The LRF shall generate a SIP 300 Multiple Choices response with the Contact header set per 8.5.2.1 to all requests from the E-CSCF when the LRF has routing information for the E-CSCF.

If the LRF supports location retrieval by an emergency Location Client, then:

- The LRF shall support one or more of the protocols defined in Clause 8.1.1 for the Le reference point.
- The LRF shall cache the Reference Identifier, UE information, and location information for the duration of the emergency call.

8.5.2.1 Header Usage

This clause discusses headers used in the SIP 300 Multiple Choices response to the E-CSCF.

Contact Header

The LRF shall set the Contact header of the redirecting response to the URI returned from the RDF. If the LRF is unable to acquire a location to associate with the call (so that it does not have sufficient information to query the RDF), or the LRF does not receive a URI in a response from the RDF, the LRF shall populate the Contact header with a default URI. The URI populated in the Contact header is a sip URI with user=phone denoting the legacy emergency services network, or a sip URI (without user=phone) denoting an ESInet.

Based on the response from the RDF (or the configured default Route URI), the LRF determines the appropriate information that is provided to the Selective Router.

If the call is to be routed to a legacy emergency services network, and the Selective Router requires the delivery of a Reference Identifier only, the LRF shall generate a Reference Identifier and set the P-Asserted-Identity header parameter in the Contact URI of the SIP 300 Multiple Choices response to this value. The P-Asserted-Identity header parameter shall also include the cpc and oli parameters. The scheme in the P-Asserted-Identity value will be of the form “sip:”.

If the call is to be routed to a legacy emergency services network and the Selective Router requires the delivery of both the callback number and a Reference Identifier, the LRF shall generate a Reference Identifier and include it as a header parameter with parameter name “Geolocation” in the Contact header field of the SIP 300 Multiple Choices response. The LRF shall also include a header parameter with parameter name “Geolocation-Routing”, that contains a value of “no” in the Contact URI of the SIP 300 Multiple Choices response, and, optionally, the “P-Asserted-Identity” header parameter that contains the callback number along with the cpc and oli parameters.

If the call is to be routed to a legacy emergency services network and the Selective Router requires the delivery of a P-Charge-Info value that was not provided in the original SIP INVITE message (e.g., the legacy Selective Router expects a Charge Number that is the same as the Reference Identifier), the LRF shall include a header parameter with parameter name “P-Charge-Info” in the Contact URI of the SIP 300 Multiple Choices response. The value of the P-Charge-Info header parameter shall be set to the value expected by the legacy Selective Router.

If the call is to be routed to an ESInet and location-by-reference is to be returned, the LRF shall generate a Reference Identifier and shall include header URI parameters in the Contact header field of the SIP 300 Multiple Choices response as specified in 3GPP TS 24.229 [Ref 2], Clause 5.12.2 6a.

If the call is to be routed to an ESInet and location-by-value is to be returned, the LRF shall generate header URI parameters in the Contact header field of the SIP 300 Multiple Choices response as specified in 3GPP TS 24.229 [Ref 2], Clause 5.12.2 6b.

If the call is to be routed to an ESInet and, per LRF-100, Additional Call Data is to be returned, the LRF shall generate header URI parameters in the Contact header field of the SIP 300 Multiple Choices response to support the return of Additional Call Data [Ref 26]. These header parameters will consist of the following:

- If Additional Call Data is to be returned “by-reference”, a “Call-Info” header field that contains an HTTPS URI and a Purpose parameter of “EmergencyCallData”.
- If Additional Call Data is to be returned “by-value”:
    - A “Call-Info” header field with CID value associated with the Additional Call Data “by-value” in the message-body and a Purpose parameter of “EmergencyCallData”.

- A header field with hname “body” and with a value that contains an escape coded MIME body of multipart/mixed MIME type containing:
  - The MIME body from the received request.
  - The Additional Call Data data structures, formatted as described in IETF RFC 7852.

- A Content-Type header field with multipart/mixed MIME type.

Note that if the LRF determines that the call is to be forwarded to an ESInet and both location-by-value and Additional Call Data “by-value” are to be included in the SIP 300 Multiple Choices response, the header field with hname “body” will contain the MIME body from the received request, a PIDF-LO, and the Additional Call Data data structure(s).

Examples:

Example for specifying a legacy emergency services network when the ALI has the fixed line location:

```
Contact: <sip:+17735554321@service.provider.net;user=phone>
```

When the ALI has the fixed line location, the LRF may not include the PAI header parameter in the Contact header of SIP 300 Multiple Choices message.

Example for specifying a legacy emergency services network with delivery of Reference Identifier and callback number. In this example, the Reference Identifier has a value of 5551234567 and a callback number of +1-707-447-6644.

```
Contact: <sip:+17735554321@service.provider.com;user=phone?
Geolocation-Routing=no&
Geolocation=<sip:+15551234567@serviceprovider.com>&
P-Asserted-Identity=sip:+17074476644;
cpc=emergency;oli=00@carrier.example.net;user=phone>
```

Example for specifying a legacy emergency services network with delivery of Reference Identifier only. In this example, the Reference Identifier has a value of 5551234567.

```
Contact: <sip:+17735554321@service.provider.com;user=phone?
P-Asserted-Identity=sip:+15551234567;
cpc=emergency;oli=00@carrier.example.net;user=phone>
```

Example for specifying an ESInet with location-by-reference.

```
Contact: <sip:esrp.esinetprovider.com?
  Geolocation-Routing=yes&
Geolocation=<https://lis.example.com/jh39udxjn3jnxpo33wn>>
```

Example for specifying an ESInet with location-by-value:

```
Contact:<sip.esrp.esinetprovider.com?Geolocation-
Routing%3Dyes%26Geolocation%3D%3Ccid%3Dtarget123%40someoperator.example.com%3E%26bod
y%3D--boundary1%0D%0A%0D%0AContent-
Type%3A%20application%2Fsdp%0D%0A%0D%0Av%3D0%0D%0Ao%3DUserA%202890844526%20289084452
6%20IN%20IP4%20here.com%0D%0As%3DSession%20SDP%0D%0Ac%3DIN%20IP4%20pc33.someoperator
.com%0D%0At%3D0%200%0D%0Am%3Daudio%2049172%20RTP%2FAVP%200%0D%0Aa%3Drtpmap%3A0%20PCM
U%2F8000%0D%0A%0D%0A--boundary1--
%0D%0A%0D%0A%3C%3Fxml%20version%3D%221.0%22%20encoding%3D%22UTF-
8%22%3F%3E%3Cpresence%20xmlns%3D%22urn%3Aietf%3Aparams%3Axml%3Ans%3Apidf%22%20xmlns%
3Agp%3D%22urn%3Aietf%3Aparams%3Axml%3Ans%3Apidf%3Ageopriv10%22%20xmlns%3Agbp%3D%22ur
n%3Aietf%3Aparams%3Axml%3Ans%3Apidf%3Ageopriv10%3AbasicPolicy%22%20xmlns%3Acl%3D%22u
```

rn%3Aietf%3Aparams%3Axml%3Ans%3Apidf%3Ageopriv10%3AcivicAddr%22%20xmlns%3Agml%3D%22h
ttp%3A%2F%2Fwww.opengis.net%2Fgml%22%20xmlns%3Adm%3D%22urn%3Aietf%3Aparams%3Axml%3An
s%3Apidf%3Adata-
model%22%20entity%3D%22pres%3Aalice.example.com%22%3E%3Ctuple%20id%3D%22target123-
1%22%3E%3Cstatus%3E%3Cgp%3Ageopriv%3E%3Cgp%3Alocation-
info%3E%3Ccl%3AcivicAddress%3E%3Ccl%3Acountry%3EUS%3C%2Fcl%3Acountry%3E%3Ccl%3AA1%3E
CA%2Fcl%3AA1%3E%3Ccl%3AA3%3EVacaville%3C%2Fcl%3AA3%3E%3Ccl%3ARD%3EQuincy%3C%2Fcl%3AR
D%3E%3Ccl%3ASTS%3ECourt%3C%2Fcl%3ASTS%3E%3Ccl%3AHNO%3E222%3C%2Fcl%3AHNO%3E%3Ccl%3APC
%3E95687%3C%2Fcl%3APC%3E%3C%2Fcl%3AcivicAddress%3E%3C%2Fgp%3Alocation-
info%3E%3Cgp%3Ausage-rules%3E%3Cgbp%3Aretransmission-
allowed%3Efalse%3C%2Fgbp%3Aretransmission-allowed%3E%3Cgbp%3Aretention-
expiry%3E2011-11-14T20%3A00%3A00Z%3C%2Fgbp%3Aretention-expiry%3E%3C%2Fgp%3Ausage-
rules%3E%3Cgp%3Amethod%3EWiremap%3C%2Fgp%3Amethod%3E%3C%2Fgp%3Ageopriv%3E%3C%2Fstatu
s%3E%3C%2Ftuple%3E%3C%2Fpresence%3E%0D%0A--boundary1--%0D%0A>

Content-Type Header

This header is used to present the body of the message, which may contain a location-by-value and/or Additional Call Data that will be used by the ESInet to route the emergency call.

Example:

```
Content-Type: multipart/mixed; boundary=boundary1
```

8.5.3 Procedures at the RDF

The RDF will receive a location from the LRF and return a Route URI that may be used to route the call to either the legacy emergency services network or an ESInet.

The RDF shall return a sip URI with “user=phone” for calls that are to be routed to a PSAP via a legacy Selective Router. This URI must be routable through the originating network and be sufficient to get the call routed over the appropriate trunk group to the Selective Router.

The RDF shall return a sip URI for calls that are to be routed to a PSAP served by the ESInet. The sip URI shall route to the ingress point of the ESInet.

If the RDF is unable to determine a Route URI based on the location provided in the routing request from the LRF, it should return a default Route URI to the LRF.

8.5.4 Procedures at the BGCF

The BGCF shall follow Clauses 4 and 5.6 in 3GPP TS 24.229 [Ref 2]. The BGCF shall remove its address from the Route header. The BGCF shall not change the Request URI and shall use the Request URI to determine the appropriate MGCF. The BGCF shall pass all headers and message bodies to the MGCF.

8.5.5 Procedures at the MGCF

The MGCF shall follow Clauses 4 and 5.5 in 3GPP TS 24.229 [Ref 2]. The MGCF shall use the cpc parameter in the P-Asserted-Identity header to identify this call as an emergency call. The MGCF shall populate the outgoing signaling to the legacy SR appropriately based on generic mappings from the information received in the incoming SIP INVITE message. The MGCF shall use the Request URI to determine the appropriate trunk group to the SR.

The MGCF shall support the standard SIP/ISUP interworking as defined by 3GPP TS 29.163 [Ref 28] and extended for ANSI by ATIS-1000679 [Ref 29]. Of particular interest for emergency calls are the following basic call interworking rules:

- The MGCF shall map the P-Asserted-Identity header field in the incoming SIP INVITE request to the SS7 ISUP Calling Party (CgPN) Number parameter.

- The MGCF shall map the SIP cpc and oli parameters from the received P-Asserted-Identity header field to the SS7 ISUP Calling Party's Category and SS7 ISUP Originating Line Information parameters, respectively.
- The MGCF shall map the P-Charge-Info header field in the incoming SIP INVITE request to the SS7 ISUP Charge Number parameter.
- While not specifically interworking, the MGCF shall have the ability to map the received R-URI digit string to "911" in the outgoing SS7 ISUP Called Party Number (CdPN).
- When the Geolocation-Routing header field is set to "no", the MGCF shall map the content of the Geolocation header field containing the sip URI with only digits to the SS7 ISUP Generic Digits Parameter (GDP).

The MGCF/MGW shall support interworking from SIP to CAMA MF signaling. The following interworking rules shall apply:

NOTE 1: The SIP to CAMA MF signaling may be realized through either direct interworking or interworking from SIP to ISUP and then from ISUP to CAMA MF. This is an implementation decision.

- If the MGCF receives a single P-Asserted-Identity header field and no Geolocation header field in the incoming SIP INVITE message, the MGCF/MGW shall outpulse a Called Number of the form "911" and an ANI of the form I [single info digit] plus the last 7-digits of the tel URI received in the P-Asserted-Identity parameter, with both digit streams contained between the KP and ST pulses.
- If the MGCF receives a P-Asserted-Identity header field and a Geolocation header field (with Geolocation-Routing header field set to "no") in the incoming SIP INVITE message, the MGCF/MGW shall outpulse a called number that is mapped from the Geolocation header field and an ANI of the form I [single info digit] plus the last 7-digits of the tel URI received in the P-Asserted-Identity header field, with both digit streams contained between the KP and ST pulses.

The mappings performed by the MGCF are summarized below:

Table 8.1 – SIP to SS7 Interworking

SIP Header	SS7 Parameter	Value
P-Asserted-Identity	Calling Party Number	Callback Number or Reference Identifier
Geolocation	Generic Digits	Reference Identifier
P-Charge-Info	Charge Number	Billing Number, Callback Number or Reference Identifier
Request-URI[12]	Called Party Number	"911"

The mappings performed by the MGCF/MGW are summarized below:

[12] Regardless of the digits contained in the Request-URI, the SS7 Called Party Number parameter will always be set to the digits "911".

Table 8.2 – SIP to CAMA/Feature Group D MF Interworking

SIP Header	MF	Value
P-Asserted-Identity	7/10-digit ANI	Callback Number or Reference Identifier
Geolocation	Called Number	Reference Identifier
Request-URI[13]	Called Number	"911"

If a trunk failure or SR failure for the primary route occurs, the MGCF will select an alternate route if available. When the MGCF cannot route the call forward, the MGCF should return a SIP 500 Server Internal Error message, per RFC 3261 [Ref 33]. The E-CSCF will then alternate route the call (per Clause 5.11.3 of TS 24.229 [Ref 2]).

8.5.6 Procedures at the IBCF

The IBCF shall follow Clauses 4 and 5.10 in 3GPP TS 24.229 [Ref 2] with the clarifications specified in Clause 6.3 of this document. If the originating IMS network supports caller identity authentication, the exit IBCF will be responsible for interacting with an STI-AS for signing of caller identity and RPH information associated with an emergency call, and populating Identity header fields associated with the caller identity and RPH in the outgoing SIP INVITE message, as described in Clauses 6.4, 7.4.2, and 8.1.2 of this document. The IBCF shall remove any "verstat" information that is present in the P-Asserted-Identity or From header fields before forwarding the SIP INVITE message to the interconnecting i3 ESInet/NGCS.

The IBCF shall use the Route header in the received SIP INVITE message to send the call to the ingress point of the ESInet. The IBCF shall pass all headers (including P headers) and message bodies unless passing of the parameters is prohibited with its role as a border gateway function. The IBCF shall ensure that the Replaces option tag is omitted from the Supported header of a SIP INVITE message associated with an emergency call that is sent to the ESInet.

8.5.7 Procedures at the P-CSCF

The P-CSCF shall follow Clauses 4 and 5.2 in 3GPP TS 24.229 [Ref 2], with the clarifications specified in Clause 6.3 of this document. If the originating IMS network supports caller identity authentication, the P-CSCF shall also follow the procedures described in Clauses 6.4 and 7.4.1 of this document.

8.5.8 Procedures at the S-CSCF

The S-CSCF shall follow Clauses 4 and 5.4 in 3GPP TS 24.229 [Ref 2].

8.5.9 Procedures at the EATF

The EATF shall follow Clause 4 in 3GPP TS 24.229 [Ref 2] and 3GPP TS 24.237 [Ref 27].

8.5.10 Procedures at the UE

The UE shall follow Clauses 4 and 5.1 in 3GPP TS 24.229 [Ref 2].

[13] If no Geolocation header is received by the MGCF in the incoming SIP INVITE message, the MGCF will signal the digits "911" as the MF Called Number.

8.5.11 Procedures for the Location Server

The LS shall support one or more of the protocols specified in Clause 8.1.1 for the L0 reference point.

If the network supports mobile emergency calls with control plane location services that uses MLP [Ref 8] as the protocol on the L0 reference point, the LS shall support the reception of location requests and sending of location responses and location reports as in Clause 6.2 and Annex B.

8.6 Media Considerations for Delivering Multimedia Calls

3GPP TS 26.114 [Ref 37] is used as the normative reference for delivering multimedia calls of type voice, GTT and video. While 3GPP TS 26.114 [Ref 37] is not specific to emergency services, it can be used as a reference by extrapolating network interfaces to legacy emergency services networks and ESInets.

RFC 4975 [Ref 38] and RFC 4976 [Ref 39] are normative references for delivering the type of media of text and pictures. This clause describes relevant clauses of each standard or RFC. The MSRP RFCs were developed to specify a protocol for transmitting instant messages in the context of a session. It is used in this standard as a replacement for SMS and the delivery of static pictures.

8.6.1 Considerations for Delivering Voice Media

Clause 5.2.1 of TS 26.114 [Ref 37] defines Codec use for terminals offering speech communications. For narrowband speech it specifies AMR speech Codecs and allows for a subset of modes and states "…{AMR-WB12.65, AMR-WB8.85 and AMR-WB6.60} should be used unless the session-setup negotiation determines that other codec modes shall be used." It is up to bilateral negotiation whether the network should pass AMR or transcode to other voice media types (e.g., G.711) prior to passing the request to the emergency services network.

The following is an example from TS 26.114 [Ref 37] of the SDP offer for negotiating voice using AMR.

```
m=audio 49152 RTP/AVP 97 98
a=tcap:1 RTP/AVPF
a=pcfg:1 t=1
a=rtpmap:97 AMR/8000/1
a=fmtp:97 mode-change-capability=2; max-red=220
a=rtpmap:98 AMR/8000/1
a=fmtp:98 mode-change-capability=2; max-red=220; octet-align=1
a=ptime:20
a=maxptime:240
```

8.6.2 Considerations for Delivering Real Time Video Media

Clause 5.2.2 of TS 26.114 [Ref 37] defines Codec use for terminals offering video communications.

"It requires the support of H.264 (AVC) [24] Constrained Baseline Profile (CBP) Level 1.2. It states that the network should support H.264 (AVC) [24] Constrained Baseline Profile Level 3.1 and H.265 (HEVC) [119] Main Profile, Main Tier, Level 3.1".

8.6.3 Considerations for Delivering GTT Media

Clause 5.2.3 of TS 26.114 [Ref 37] defines Codec use for terminals offering real time text communications. It specifies the use of ITU-T T.140 [Ref 40].

The following is an example from TS 26.114 [Ref 37] of the SDP offer for negotiating real time text.

```
m=text 53490 RTP/AVP 100 98
b=AS:2
b=RS:0
b=RR:500
a=rtpmap:100 red/1000/1
a=rtpmap:98 t140/1000/1
a=fmtp:100 98/98/98
```

8.6.4 Considerations for Delivering Text Media

Clause 13a of TS 26.114 [Ref 37] defines the use of MSRP for messaging and video. This clause defines the use of MSRP for session-mode messaging that exchanges text media during a SIP session. RFCs 4975 [Ref 38] and 4976 [Ref 39] are referenced in this standard to define the exchange of text media to 9-1-1.

> NOTE: MSRP session-mode can be interworked to Baudot tones, although a standard is not yet defined to do the interworking.

Video calls shall use the procedures defined in Clause 8.6.2 of this standard.

Clause 8 of RFC 4975 [Ref 38] defines connection management and SDP parameter usage in the negotiation of MSRP via the SIP offer/answer mechanism. The forking of SIP requests is not supported for emergency services. This standard only supports point to point connections, i.e., caller to/from the Telecommunicator.

The following is an example from RFC 4975 [Ref 38] of the SDP offer for negotiating session-mode messaging.

```
c=IN IP4 atlanta.example.com
m=message 7654 TCP/MSRP *
a=accept-types:text/plain
a=path:msrp://atlanta.example.com:7654/jshA7weztas;tcp
```

RFC 4976 [Ref 39] only applies if the network uses MSRP relays. With RFC 4976 extensions [Ref 39], MSRP clients can communicate directly, or through an arbitrary number of relays. Each client is responsible for identifying any relays acting on its behalf and providing appropriate credentials. Using this RFC, clients that can receive new TCP connections directly do not have to implement any new functionality to work with these relays.

8.7 Stage 3 Call Flows

The call flows in this clause provide definition for the LRF, RDF, and LS. They represent specific use cases enumerated in this document. They show calls being delivered to either a legacy Selective Router or an ESRP in the ESInet.

8.7.1 Routing Fixed UE to a Legacy Network Based upon Network Acquired Location (Dual Hosted Location Information Scenario)

The flow in Figure 8.9 illustrates a UE in a fixed location initiating the emergency call, the network acquiring the location, the network using that location to determine the route, and the network routing the call to the legacy emergency network. In this example, the UE is associated with a Telephone Number (TN) which is represented as an E.164 number in the figure. This flow assumes that there is location information hosted in the LS to route the call to the Selective Router and that the location displayed to the PSAP is hosted in the ALI of the legacy emergency services network.

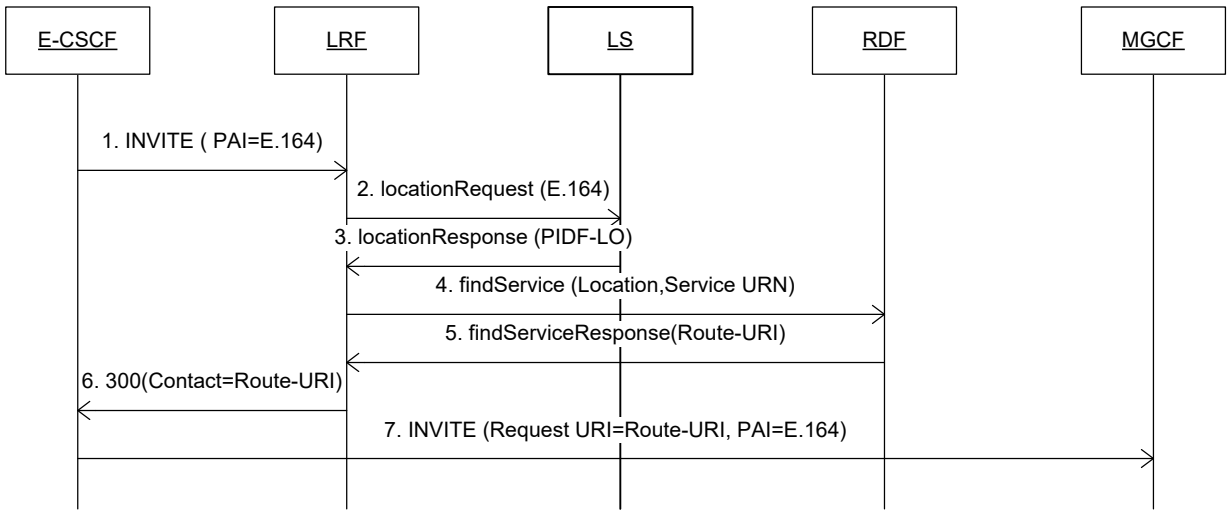

Figure 8.9 - Fixed UE Routed to Legacy using Network Provided Location Passing TN

Step 1. The E-CSCF forwards the SIP INVITE to the LRF, passing all headers and message body received from the P-CSCF.

Step 2. The LRF needs to acquire the location (e.g., using HELD with identity extensions [Ref 10]) and sends a locationRequest to the LS passing the TN, which is represented as an E.164 number.

Step 3. The LS acquires the location associated with the TN and returns a locationResponse containing PIDF-LO to the LRF with the location.

Step 4. The LRF needs to acquire location-based routing information and takes the PIDF-LO and formats it for the query to the RDF. The LRF sends a findService request to the RDF passing the Location and Service URN.

Step 5. The RDF responds with a findServiceResponse that includes the Route URI.

Step 6. The LRF formats a SIP 300 Multiple Choices response that includes the Route URI in the Contact header.

Step 7. The call is routed from E-CSCF towards the MGCF.

8.7.2 Routing Fixed UE to a Legacy Network Based upon Network Acquired Location (Single Location Information Scenario)

The flow in Figure 8.10 illustrates a UE in a fixed location initiating the emergency call, the network acquiring the location, the network using that location to determine the route, the network assigning a Reference ID, and the network routing the call to the legacy emergency network. In this example, the UE is associated with a Telephone Number (TN) which is represented as an E.164 number in the figure. This flow assumes that the caller location resides in the LS and is used by the originating network to route the call. The Reference Identifier is created and passed to the legacy emergency services network and used by that network to route the call and to query the LRF for location. This scenario assumes ALI redirection (shell records) and allocation of additional Reference Identifiers.

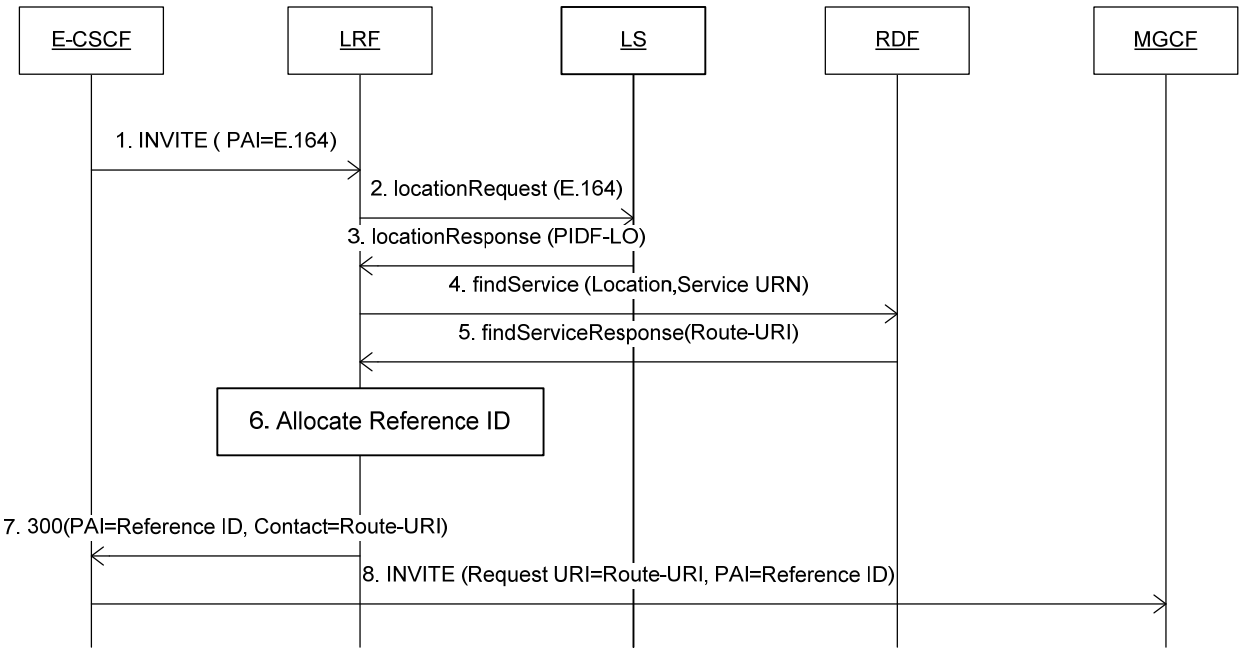

Figure 8.10 – Fixed UE Routed to Legacy using Network Provided Location Passing Reference ID

Step 1. The E-CSCF forwards the SIP INVITE to the LRF, passing all headers and message body received from the P-CSCF.

Step 2. The LRF needs to acquire the location (e.g., using HELD with identity extensions [Ref 10]) and sends a locationRequest to the LS passing the TN, which is represented as an E.164 number.

Step 3. The LS acquires the location associated with the TN and returns a locationResponse containing PIDF-LO to the LRF with the location.

Step 4. The LRF needs to acquire location-based routing information and takes the PIDF-LO and formats it for the query to the RDF. The LRF sends a findService request to the RDF passing the Location and Service URN.

Step 5. The RDF responds with a findServiceResponse that includes the Route URI.

Step 6. The LRF recognizes that the call is destined to a legacy emergency services network based upon the format of the response from the RDF, caches the location information, and creates a Reference Identifier that may be used by the emergency services network to retrieve the location.

Step 7. The LRF formats a SIP 300 Multiple Choices response that includes the Reference ID in the PAI header and the Route URI in the Contact header.

Step 8. The call is routed from the E-CSCF towards the MGCF.

8.7.3 Routing Fixed UE to an ESInet based upon Network Acquired Location

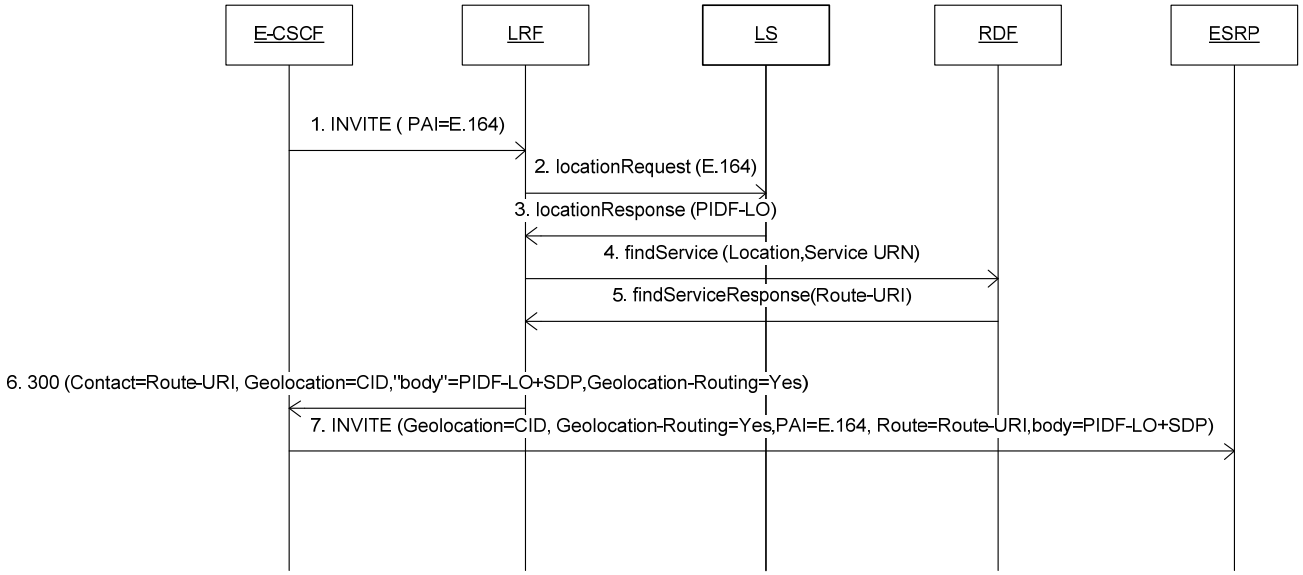

Figure 8.11 – Fixed UE Routed to ESInet using Network Provided Location

Step 1. The E-CSCF forwards the SIP INVITE to the LRF, passing all headers and message body received from the P-CSCF.

Step 2. The LRF needs to acquire the location (e.g., using HELD with identity extensions [Ref 10]) and sends a locationRequest to the LS passing the TN, which is represented as an E.164 number in the flow.

Step 3. The LS acquires the location associated with the TN and returns a locationResponse containing PIDF-LO to the LRF.

Step 4. The LRF needs to acquire location-based routing information and takes the PIDF-LO and formats it for the query to the RDF. The LRF sends a findService request to the RDF passing the Location and Service URN.

Step 5. The RDF responds with a findServiceResponse that includes the Route URI. The Route URI will point to the ESRP via the IBCF (not shown).

Step 6. The LRF formats a SIP 300 Multiple Choices response that includes a Contact header with the Route URI. Recognizing that the call is destined to an ESInet based upon the format of the response from the RDF, the LRF formats a SIP 300 Multiple Choices response as specified in Clause 8.5.2.

Step 7. The E-CSCF copies needed parameters returned in the Contact header of the SIP 300 Multiple Choices response to the outgoing SIP INVITE as specified in Clause 8.5.1 for a call destined for an ESInet.

8.7.4 Routing a UE Provided Location to the Legacy Emergency Services Network

Figure 8.12 illustrates the situation where the UE can pass its location (i.e., PIDF-LO) in the SIP INVITE. The call is routed to a legacy emergency services network. Since this location cannot be passed to the legacy emergency services network, the network must cache it and assign a Reference Identifier. This Reference Identifier is passed to the legacy emergency services network to allow it to retrieve the UE location.

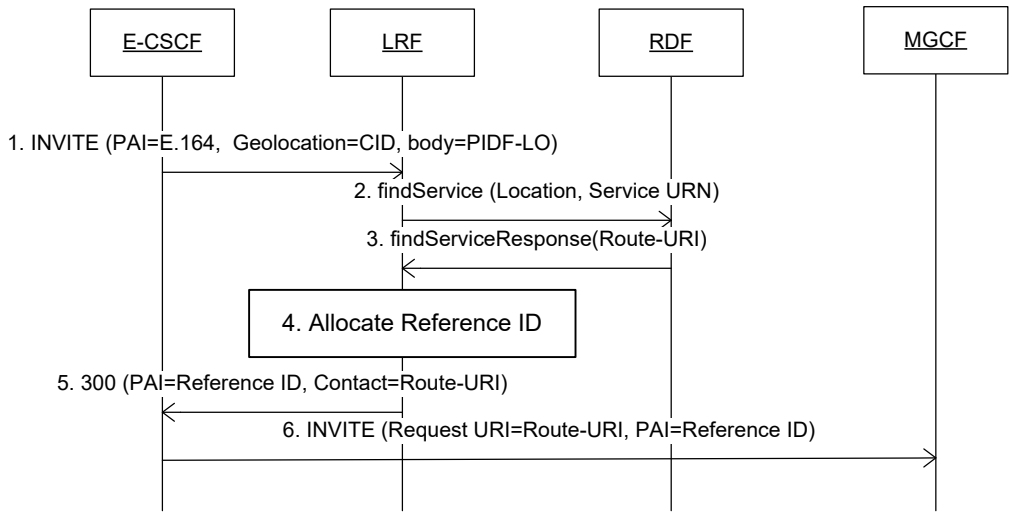

Figure 8.12 - UE Provided Location to Legacy

Step 1. The E-CSCF forwards the INVITE to the LRF, passing all headers and message body received from the P-CSCF. The Geolocation header will contain a CID that points to the PIDF-LO in the message body. The message body contains SDP and PIDF-LO.

Step 2. The LRF recognizes that the location is already available and it only needs to acquire location-based routing information. It takes the PIDF-LO and formats it for the query to the RDF. It sends a findService request to the RDF passing the Location and Services URN.

Step 3. The RDF responds with a findServiceResponse that includes the Route URI.

Step 4. The LRF recognizes that the call is destined to a legacy emergency services network based upon the format of the response from the RDF, caches the location information, and creates a Reference Identifier that may be used by the emergency services network to retrieve the location.

Step 5. The LRF formats a SIP 300 Multiple Choices response that includes the Reference Identifier in the PAI header and the Route URI in the Contact header.

Step 6. The E-CSCF copies the PAI header parameter in the Contact header of the SIP 300 Multiple Choices response to the PAI header of the outgoing INVITE.

8.7.5 Routing a UE Provided Location to the ESInet

Figure 8.13 illustrates the situation where the fixed line UE can pass its location (i.e., PIDF-LO) in the SIP INVITE and the call is routed to an ESInet. Since the ESInet is capable of receiving the location information, the network does not need to assign a Reference Identifier. It must just choose a route to the ESInet.

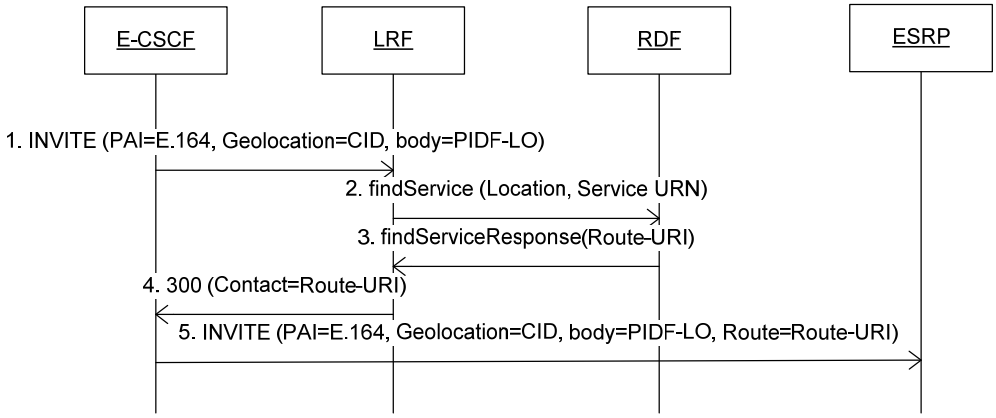

Figure 8.13 - UE Provided Location to ESInet

Step 1. The E-CSCF forwards the INVITE to the LRF, passing all headers and message body received from the P-CSCF. The Geolocation header will contain a CID that points to the PIDF-LO in the message body. The message body contains SDP and PIDF-LO.

Step 2. The LRF recognizes that the location is already available and it only needs to acquire location-based routing information. It takes the PIDF-LO and formats it for the query to the RDF. It sends a findService request to the RDF passing the Location and the Service URN.

Step 3. The RDF responds with a findServiceResponse that includes the Route URI. The Route URI will point to the ESRP via the IBCF (not shown).

Step 4. The LRF recognizes that the call is destined to an ESInet based upon the format of the response from the RDF, and because it received a PIDF-LO in the INVITE does not assign a Reference Identifier. The LRF formats a SIP 300 Multiple Choices response that includes the Route URI in the Contact header.

Step 5. The E-CSCF uses the Route header to route the call to the ESRP via the IBCF (not shown).

8.7.6 Initial Location Request

Figure 8.14 and Figure 8.15 show the query from the emergency location services (LCS) client which may be either the legacy ALI database or a functional element in the ESInet. This request is for a low time delay/initial response, which means that the LRF responds with whatever information it has at the time. For a mobile call, this may be the cell site address representing Phase 1 location information or, if Phase 2 location has been acquired, it may be the location of the UE. If the initial request is not for a low time delay response, the flow may follow the one illustrated in Clause 8.6.7.

Figure 8.14 shows the flow from a legacy emergency services network (i.e., the ALI) using the E2 message of ESPOSREQ. Other legacy protocols can be extrapolated.

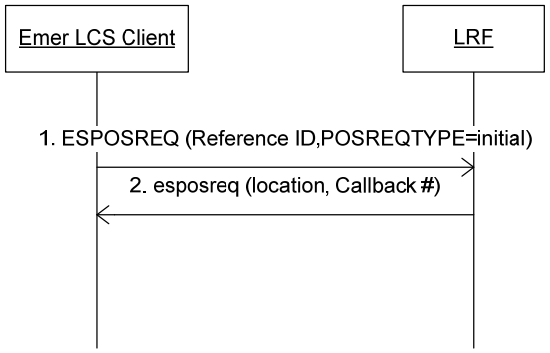

Figure 8.14 – Initial Location Request from Legacy Emergency Services Network

Step 1. The emergency LCS client (i.e., the ALI) issues an ESPOSREQ to the LRF with the Reference ID (i.e., ESRK) that was provided in the call request. Position Request Type is set to “initial”.

Step 2. The LRF retrieves location information that is available at the time of the request and returns it along with the callback number.

Figure 8.15 shows an initial query from an ESInet with the dereferencing protocol using HELD. The query is from a functional element such as a PSAP or ESRP.

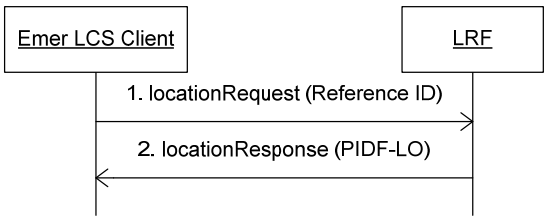

Figure 8.15 – Initial Query from ESInet

Step 1. The emergency LCS client (e.g., NENA i3 PSAP) queries the LRF with the Reference Identifier provided in the call request.

Step 2. The LRF retrieves location information that is available at the time of the request and returns it.

8.7.7 Update Location Request

When the emergency LCS client (i.e., the ALI) requests an updated location, or when the initial location request has high time delay, the flows in Figure 8.16 and Figure 8.17 apply. In Figure 8.16 for legacy emergency services network, this flow shows an E2 ESPOSREQ request from the emergency LCS client and MLP from the LRF. Other protocols can be extrapolated.

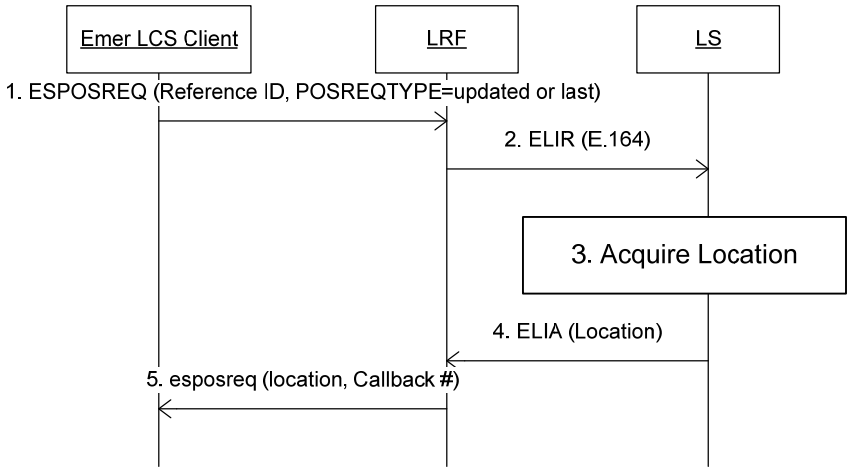

Figure 8.16 – Update Location Request from Legacy Emergency Services Network shown as MLP interaction

Step 1. The legacy emergency LCS client (i.e., the ALI) issues an ESPOSREQ to the LRF with the Reference Identifier (i.e., ESRK) that was provided in the call request. Position Request Type is set to “updated or last known”.

Step 2. The LRF initiates the location acquisition process by sending a Mobile Location Protocol (MLP) Emergency Location Immediate Request (ELIR) message to the LS passing the E.164 number associated with the Reference Identifier.

Step 3. The network implements procedures for location acquisition. If the LRF has a core network entity identity cached, the LRF will include it in the ELIR.

Step 4. At some point, the location has been acquired and the LS responds back to the LRF with a MLP Emergency Location Immediate Answer (ELIA) message with the location.

Step 5. The LRF returns the location information to the legacy client along with the callback number in an esposreq response.

NOTE: If the LS failed to obtain location (e.g., a handover to another Core Network Entity occurred), the LS may return a failure indication to the LRF in Step 4 and include the target core network entity identity.

The ESInet flow illustrated in Figure 8.17 uses the dereferencing protocol using HELD.

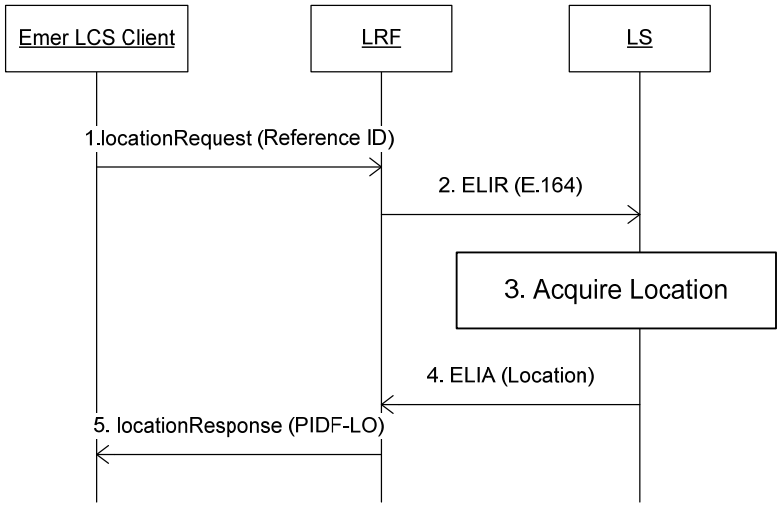

Figure 8.17 – Update Location Request from ESInet shown as MLP interaction

Step 1. The ESInet client (e.g., the PSAP) issues a deference request using HELD to the LRF with the Reference Identifier provided in the call request.

Step 2. The LRF initiates the location acquisition process by sending a MLP ELIR to the LS passing the E.164. If the LRF has a core network entity identity cached, the LRF will include it in the ELIR.

Step 3. The network implements procedures for location acquisition.

Step 4. At some point, the location has been acquired and the LS responds back to the LRF with a MLP ELIA message with the location.

Step 5. The LRF returns the PIDF-LO to an ESInet client in a HELD locationResponse.

NOTE: If the LS failed to obtain location (e.g., a handover to another Core Network Entity occurred), the LS may return a failure indication to the LRF in Step 4 and include the target core network entity identity.

8.7.8 Emergency Location Report

When control plane location service is used in a network for mobile IMS emergency calls, location continuity is required (see Annex C.1.5). Based on configuration, the source or target core network entity (e.g., MME, SGSN, MSC) reports a change in serving core network entity to the LS when the UE moves to another core network entity in the access network. The LS forwards the report to the LRF. It should be noted that a control plane location service may be used in a source core network but not in a target core network or vice versa. In such a case, the change in serving core network entity may have to be reported by the core network that supports the control plane location service.

The serving core network entity may also send a report to the LS when emergency bearer service is created or terminated.

MLP Emergency Location Report (ELR) [Ref 8] is used on the L0 interface to forward the report to the LRF.

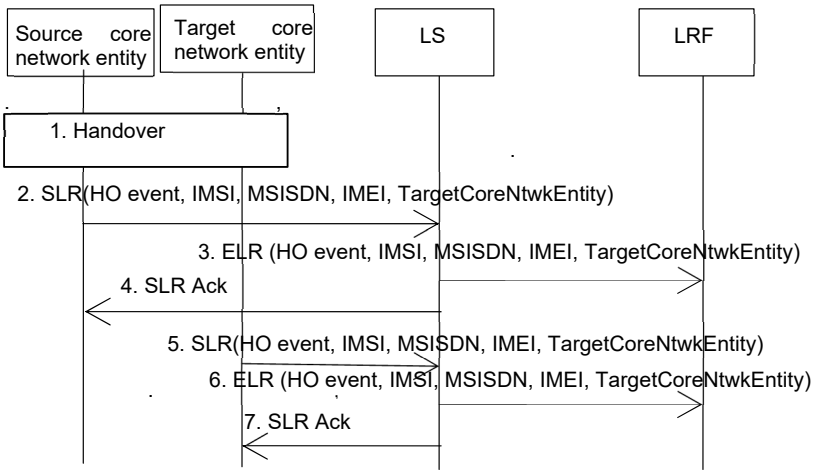

Figure 8.18 – Emergency Location Report

Step 1. While a UE has emergency bearer service active, a handover from a source core network entity (e.g., MME, SGSN, MSC) to a different target core network entity occurs.

Step 2. If the core network entity is configured to report the event at the source core network entity, the source core network entity reports the target core network entity to the LS and includes the event type and UE identity.

Step 3. The LS reports the event to the LRF in an MLP Emergency Location Report. The LRF uses implementation-specific mechanisms (e.g., mapping core network entity to LS) to determine the LS that serves the target entity.

Step 4. The LS acknowledges the report from the source core network entity.

Step 5. If the core network entity is configured to report the event at the target core network entity, the target core network entity reports the target core network entity to the LS and includes the event type and UE identity. Note that the LS receiving the SLR may be different than the LS associated with the source core network entity.

Step 6. The LS reports the event to the LRF in an MLP Emergency Location Report. The LRF uses implementation-specific mechanisms (e.g., mapping core network entity to LS) to determine the LS that serves the target entity.

Step 7. The LS acknowledges the report from the target core network entity.

9 Access Network Requirements

This clause describes any differences to existing standards, including use of particular options regarding treatment of different access types for support of IMS Emergency Calls in North America.

9.1 LTE Access

A UE with LTE access shall always establish an emergency PDN connection for a UE detectable emergency session as defined in 3GPP TS 23.167, Annex H [Ref 1]. The option defined in 3GPP TS 24.229 [Ref 2], Clause 5.1.6.1, of establishing an IMS emergency call in the home network using a normal PDN connection and normal IMS registration is not supported in this standard with LTE access.

For LTE access, an originating network and UE shall support IMS emergency calls for all types of limited service state as identified by category (d) (“all UEs are allowed”) in 3GPP TS 23.401 [Ref 14], Clause 4.3.12.1.

9.2 HSPA Access

A UE with HSPA access shall always establish an emergency Packet Data Protocol PDP context for a UE detectable emergency session as defined in 3GPP TS 23.167, Annex H [Ref 1]. The option defined in 3GPP TS 24.229 [Ref

2], Clause 5.1.6.1, of establishing an IMS emergency call in the home network using a normal PDP context and normal IMS registration is not supported in this standard with HSPA access.

For HSPA access, an originating network and UE shall support IMS emergency calls for all types of limited service state as identified by category (d) (“all UEs are allowed”) in 3GPP TS 23.401 [Ref 14], Clause 4.3.12.1.

Annex A
(normative)

A SIP INVITE Profile for Emergency Calls

This normative annex provides the SIP INVITE profile for emergency calls between the IBCF in the originating network and the BCF in the next generation emergency services network (ici reference point). Headers mentioned in 3GPP TS 24.229 [Ref 2] and not included in this table are not pertinent to emergency calls and may be ignored.

Table A.1 – Profile Legend

Code	Code name	Sending side	Receiving side
M	Mandatory	The capability shall be supported. It is a static view of the fact that the conformance requirements related to the capability in the reference specification are mandatory requirements. This does not mean that a given behavior shall always be observed, but that it shall be observed when the implementation is placed in conditions where the conformance requirements from this document compel it to do so. For instance, if the support for a header in a sent request or response is mandatory, it does not mean that it shall always be present, but that it shall be present according to the description of the behavior in this document.	Same as in the sending side with the following additions: • Processing should not continue if required information is unavailable. (Suitable disconnection/release processing should be performed.) • However, when a default value has been decided upon, processing is performed using the default value.
O	Optional	The capability may or may not be supported. It is an implementation choice.	Same as in the sending side with the following additions: • If possible, perform the processing expected by the sending side. • When the processing expected by the sending side cannot be performed, the received content should be ignored and processing should continue.
-	Not Supported	The capability is not supported or beyond the scope of this standard.	The capability is not supported or beyond the scope of this standard.
S	Recommended	The capability should be supported. It is an implementation choice.	Same as in the sending side with the following additions: • If possible, perform the processing expected by the sending side. • When the processing expected by the sending side cannot be performed, the received content should be ignored and processing should continue.

Table A.2 – SIP INVITE Header Profile

Header	Send	Recv	Reference and Notes
Accept	M	M	RFC 3261 [Ref 33] Clause 20.1. Conditional in 3GPP TS 24.229 [Ref 2].
Accept-Encoding	O	M	RFC 3261 [Ref 33], Clause 20.2.
Accept-Language	S	M	RFC 3261, Clause 20.3. The “Accept-Language” header *should* be present in requests with a value of “en” for English, which *shall* be supported. Other values MAY be supported. Send optional in TS 24.229 [Ref 2].
Alert-Info	O	O	RFC 3261 [Ref 33], Clause 20.4. Receive conditional in 3GPP TS 24.229 [Ref 2].
Allow	M	M	RFC 3261 [Ref 33], Clause 20.5. The header value *shall* list all supported methods – i.e., at a minimum, “INVITE”, “ACK”, “CANCEL”, “BYE”, “OPTIONS”, and “PRACK”. The “Allow” header *shall* be present in the initial SIP INVITE and the SIP 200 OK response to the initial SIP INVITE. However, the BCF *should* be prepared to receive messages without the Allow header field. The BCF *should* continue the call control even if the Allow header is not present in the initial SIP INVITE and the IBCF *should* continue the call control from the 2xx response to the initial SIP INVITE. Send optional in 3GPP TS 24.229 [Ref 2].
Allow-Events	O	O	RFC 3265 [Ref 32], Clause 3.3.7. Conditional in 3GPP TS 24.229 [Ref 2].
Attestation-Info	O	O	Clause 8.2.1 of this standard. Conditional in 3GPP TS 24.229 [Ref 2].
Authentication-Info	-	-	RFC 3261 [Ref 33], Clause 20.6. Not defined in 3GPP TS 24.229 [Ref 2].
Authorization	-	-	RFC 3261 [Ref 33], Clause 20.7. Conditional in 3GPP TS 24.229 [Ref 2].
Call-ID	M	M	RFC 3261 [Ref 33], Clause 20.8.
Call-Info	O	O	RFC 3261 [Ref 33], Clause 20.9. It is noted that there are security risks associated with acting on the Call-Info header as described in RFC 3261 [Ref 33] Clause 20.9.
Contact	M	M	RFC 3261 [Ref 33], Clause 20.9. The IBCF applications *shall* populate the Contact header field in a SIP INVITE request, and the BCF *shall* populate the Contact header in a 2XX response to an SIP INVITE request, with a SIP-URI. Support for any other type of URI is OPTIONAL.
Content-Disposition	O	M	RFC 3261 [Ref 33], Clause 20.11.
Content-Encoding	O	M	RFC 3261 [Ref 33], Clause 20.12. The Content-Encoding header *shall* be used by the IBCF/BCF implementations. The "identity" encoding value *shall* be supported; other encodings *may* be supported.
Content-Language	O	O	RFC 3261 [Ref 33], Clause 20.13.

Header	Send	Recv	Reference and Notes
Content-Length	M	M	RFC 3261 [Ref 33], Clause 20.14.
Content-Type			RFC 3261 [Ref 33], Clause 20.15; RFC 6442 [Ref 30], Clause 5.1. The value of “multipart/mixed” *shall* be supported. The value of “application/sdp” *shall* be supported. The value of “application/pidf+xml” MAY be supported and *shall* be supported if location-by-value is included in the body of the SIP INVITE message.
CSeq			RFC 3261 [Ref 33], Clause 20.16.
Date			RFC 3261 [Ref 33], Clause 20.17. Send conditional, Receive mandatory in 3GPP TS 24.229 [Ref 2].
Error-Info			RFC 3261 [Ref 33], Clause 20.18. It is noted that there are security risks associated with acting on the Error-Info header as described in RFC 3261 [Ref 33], Clause 20.18. Not defined in 3GPP TS 24.229 [Ref 2].
Expires	-	-	RFC 3261 [Ref 33], Clause 20.19. Optional in 3GPP TS 24.229 [Ref 2].
From	M	M	RFC 3261 [Ref 33], Clause 20.20, and 8.5.1.1 of this standard.
Geolocation	M	M	RFC 6442 [Ref 30], Clause 4.1, and 8.5.1.1 of this standard. Conditional in 3GPP TS 24.229 [Ref 2].
Geolocation-Routing	O	O	RFC 6442 [Ref 30] Clause 4.2, and 8.5.1.1 of this standard. Not defined in 3GPP TS 24.229 [Ref 2].
History-Info	O	M	RFC 4244 [Ref 43]. Conditional in 3GPP TS 24.229 [Ref 2].
Identity	O	O	RFC 8224 [Ref 50]. Conditional in 3GPP TS 24.229 [Ref 2].
In-Reply-To	-	-	RFC 3261 [Ref 33], Clause 20.21. Optional in 3GPP TS 24.229 [Ref 2].
Max-Forwards	M	M	RFC 3261 [Ref 33], Clause 20.22. When the IBCF implementation of a back-to-back User Agent (B2BUA) forwards a request, it *shall* use a Max-Forwards value equal to the incoming Max-Forwards value minus one.
Min-Expires		-	RFC 3261 [Ref 33], Clause 20.23. Not defined in 3GPP TS 24.229 [Ref 2].
MIME-Version	O	M	RFC 3261 [Ref 33], Clause 20.24. The MIME-Version header *shall* be used by the IBCF/BCF implementations. The version "1.0" value *shall* be supported; other values *may* be supported.
Organization	-	-	RFC 3261 [Ref 33], Clause 20.25. Optional in 3GPP TS 24.229 [Ref 2].
Origination-Id	O	O	Clause 8.2.1 of this standard. Conditional in 3GPP TS 24.229 [Ref 2].
P-Access-Network-Info Header	O	O	RFC 3455 [Ref 42], Clause 4.4.1, and 8.5.1.1 of this standard. Conditional in 3GPP TS 24.229 [Ref 2].
P-Asserted-Identity	O	O	RFC 3325 [Ref 44], Clause 4, and 8.5.1.1 of this standard. n/a in Send and Conditional in Receive in 3GPP TS 24.229 [Ref 2].

Header	Send	Recv	Reference and Notes
P-Charging-Vector Header	O	O	RFC 3325 [Ref 44], Clause 4.6, and 8.5.1.1 of this standard. Conditional in 3GPP TS 24.229 [Ref 2].
Priority	-	-	RFC 3261 [Ref 33], Clause 20.26. Optional in 3GPP TS 24.229 [Ref 2].
Proxy-Authenticate	-	-	RFC 3261 [Ref 33], Clause 20.27. Not defined in 3GPP TS 24.229 [Ref 2].
Proxy-Authorization	-	-	RFC 3261 [Ref 33], Clause 20.28. Send optional and Receive conditional in 3GPP TS 24.229 [Ref 2].
Proxy-Require	-	-	RFC 3261 [Ref 33], Clause 20.29. Send optional and Receive n/a.
Record-Route	M	M	RFC 3261 [Ref 33], Clause 20.30.
Reply-To	-	-	RFC 3261 [Ref 33], Clause 20.31. Optional in 3GPP TS 24.229 [Ref 2].
Require	O	O	RFC 3261 [Ref 33], Clause 20.32. The option tags “precondition”, and “100rel” *shall* be supported.
Retry-After	-	-	RFC 3261 [Ref 33], Clause 20.33. Not defined in 3GPP TS 24.229 [Ref 2].
Route	M	M	RFC 3261 [Ref 33], Clause 20.34. Send conditional in 3GPP TS 24.229 [Ref 2].
Server	-	-	RFC 3261 [Ref 33], Clause 20.35. Not defined in 3GPP TS 24.229 [Ref 2].
Subject	-	-	RFC 3261 [Ref 33], Clause 20.36. Optional in 3GPP TS 24.229 [Ref 2].
Supported	M	M	RFC 3261 [Ref 33], Clause 20.37. The values “precondition” and “100rel” *shall* be supported. The value “replaces” *shall not* be present. However, a value present in the "Require" header *should not* also be present in the Supported header.
Timestamp	O	M	RFC 3261 [Ref 33], Clause 20.38.
To	M	M	RFC 3261 [Ref 33], Clause 20.39, and 8.5.1.1 of this standard.
Unsupported	M	M	RFC 3261 [Ref 33], Clause 20.40.
User-Agent	-	-	RFC 3261 [Ref 33], Clause 20.41. Optional in 3GPP TS 24.229 [Ref 2].
Via	M	M	RFC 3261 [Ref 33], Clause 20.42.
Warning	O	O	RFC 3261 [Ref 33], Clause 20.43.
WWW-Authenticate	-	-	RFC 3261 [Ref 33], Clause 20.44. Not defined in 3GPP TS 24.229 [Ref 2].

Annex B
(normative)

B Using MLP Between the LRF & LS for L0

Communication between the LRF and the LS over L0 is made up of two distinct information flows: a request and response flow that permits location to be requested by the LRF from the LS, and an asynchronous flow from the LS to the LRF when a control-plane LS is deployed. The examples in this annex are informative.

B.1 Request/Response Queries between LRF & LS over L0

MLP supports emergency location requests with the Emergency Location Immediate Request (ELIR) message which is defined in Clause 5.2.3.3.1 of the MLP specification [Ref 8]. This ELIR is a request for location information, but additional criteria such as quality of position and location type may also be requested.

The Emergency Location Immediate Answer (ELIA) message is sent in response to the ELIR. The ELIA is defined in Clause 5.2.3.3.2 of the MLP specification [Ref 8].

The following tables specify which elements in the ELIR must be specified in the request from the LRF to the LS.

Table B.1 – ELIR (eme_lir element)

eme_lir element	Inclusion	Description
msids	M	The identity or identities of the calling entity.
target_serving_node	C	The identity of the current serving node. This element shall be present if the location request is being made to a control-plane LS and was previously received from an LS in an ELR or ELIA.

Table B.2 – ELIR (eme_lir element)

msids	Inclusion	Description
msid	M	The identity of the calling entity. More than one may be included (e.g., IMEI and MSISDN). It is an error to include multiple msid elements of the same type. The location server must preserve all msid elements and their order from the request to the response.

Table B.3 – msid attribute values

msid type attribute	Support	Description
MSISDN	C	The MSISDN of the calling entity if available.
IMSI	C	The IMSI of the calling entity if available.
IMEI	C	The IMEI of the calling entity if available.
MIN	C	The MIN of the calling entity if available.
MDN	C	The MDN of the calling entity if available.
NOTE: Values not shown are not applicable to this standard and may be ignored by the location server.		

Table B.4 – target_serving_node element

target_serving_node element	Support	Description
vmscid	C	The identity of the MSC serving the calling entity.
mme_name	C	The identity (FQDN) of the MME serving the calling entity.
sgsn_name	C	The identity (FQDN) of the SGSN serving the calling entity.
sgsnid	C	The identity of the SGSN serving the calling entity.

The following tables specify which elements in the ELIA must be specified in the response from the LS to the LRF.

Table B.5 – ELIA (eme_lia element)

eme_lir element	Inclusion	Description
eme_pos	M	Body of the message.

Table B.6 – eme_pos element values for ELIA

eme_pos element	Support	Description
msid	M	One or more identifiers for the UE.
pd	C	A location shall be provided if it is included in the location response received by the LS.
poserr	C	Shall be included if the location response received at the LS indicates an error.
target_serving_node	C	The target_serving_node shall be provided if it is included in the location response received by the LS. See Note 1.
serving_cell	C	The serving cell shall be provided if it is included in the location response received by the LS.
NOTE 1: It is possible for a handover to occur after a location request is sent from the LS to the serving network entity and before the positioning process is completed. In this case, the ELIA message from the LS to the LRF includes the target_serving_node element containing the identity of the new serving network entity. Note that if a handover occurs and the LS is able to support retrying a position request against the new serving network entity, then it could do so and include the target_serving_node element in that response. NOTE 2: Values not shown are not applicable to this standard.		

Examples ELIR and corresponding ELIA messages are shown below:

```
<eme_lir ver="3.4.0">
      <msids>
       <msid type="MSISDN">14475552222</msid>
       <msid type="IMEI">1234567890abcde</msid>
      </msids>
      <target_serving_node>
        <vmscid>
          <vmscno>1541154871</vmscno>
        </vmscid>
      </target_serving_node>
      <loc_type type="CURRENT_OR_LAST" />
</eme_lir>


<eme_lia ver="3.4.0">
  <eme_pos>
    <msids>
       <msid type="MSISDN">14475552222</msid>
```

```
        <msid type="IMEI">1234567890abcde</msid>
    </msids>
    <pd>
      <time utc_off="0300">20121207151800</time>
      <shape>
        <CircularArea srsName="www.epsg.org#4326">
          <coord>
            <X>30 24 43.53N</X>
            <Y>45 28 09.534W</Y>
          </coord>
          <radius>25</radius>
        </CircularArea>
      </shape>
    </pd>
  </eme_pos>
</eme_lia>


<eme_lir ver="3.4.0">
      <msids>
      <msid type="MSISDN">14475552222</msid>
      <msid type="IMEI">0123456789abcde
      </msid>
      </msids>
      <target_serving_node>
        <mme_name>mme1.operatorname.pub.3gppnetwork.org</mme_name>
      </target_serving_node>
      <loc_type type="CURRENT_OR_LAST" />
</eme_lir>



<eme_lia ver="3.4.0">
  <eme_pos>
    <msids>
       <msid type="MSISDN">14475552222</msid>
        <msid type="IMEI">0123456789abcde</msid>
    </msids>
    <pd>
      <time utc_off="0300">20121207151800</time>
      <shape>
        <CircularArea srsName="www.epsg.org#4326">
          <coord>
            <X>30 24 43.53N</X>
            <Y>45 28 09.534W</Y>
          </coord>
          <radius>25</radius>
        </CircularArea>
      </shape>
    </pd>
    <target_serving_node>
      <mme_name>mme2.operatorname.pub.3gppnetwork.org</mme_name>
    </target_serving_node>
  </eme_pos>
</eme_lia>
```

B.2 Asynchronous Data Push from LS to LRF over L0

Data is pushed asynchronously from the LS to the LRF using the MLP Emergency Location Report (ELR). The ELR is defined in Clause 5.2.3.5.1 of the MLP specification [Ref 8].

Table B.7 – ELR (emerep element)

emerep element	Inclusion	Description
eme_event	M	The event responsible for triggering the report.
locationserver_address	C	When eme_trigger event is EME_ORG: the URL of the Location Server shall be included. When eme_trigger event is EME_HO: the URL of the target Location Server shall be included when the target Location Server sends the ELR. When eme_trigger event is EME_HO, the new target serving node is not handled by this LS, and the source location server sends the ELR: the locationserver_address element shall not be used.

Table B.8 – eme_event values

eme_event element/attribute	Support	Description
eme_pos	M	Body of the message caused by the trigger.
eme_trigger	M	The type of event that caused the trigger.

Table B.9 – eme_trigger values

eme_trigger attribute values	Support	Description
EME_ORG	C	Used when the LS is reporting an initial SLR event to the LRF.
EME_REL	C	Used when the LS is reporting an SLR termination (release) event to the LRF.
EME_HO	C	Used when the LS is reporting a handover SLR event to the LRF.

Table B.10 – eme_pos element values for ELR

eme_pos element	Support	Description
msid	M	One or more identifiers for the UE.
pd	C	A location must be provided if it is included in the SLR received by the LS.
poserr	O	Should not be sent to the LRF.
target_serving_node	C	For an EME_ORG event, the current serving node identity shall be included in the target_serving_node element if the serving node identity is included in the SLR received by the LS. For an EME_HO event, the target_serving_node shall be provided if it is included in the SLR received by the LS.
serving_cell	C	The serving cell shall be provided if it is included in the SLR received by the LS.
NOTE: Values not shown are not applicable to this standard.		

Table B.11 – target_serving_node element

target_serving_node element	Support	Description
vmscid	C	The identity of the MSC serving the calling entity.
mme_name	C	The identity (FQDN) of the MME serving the calling entity.
sgsn_name	C	The identity (FQDN) of the SGSN serving the calling entity.
sgsnid	C	The identity of the SGSN serving the calling entity.

Table B.12 – serving_cell element

serving_cell element	Support	Description
cgi	C	The serving CGI of the calling entity, provided if available.
sai	C	The serving cell in SAI format of the calling entity, provided if available.
(mcc, mnc, lte ci)	C	The serving cell identity when the calling entity is on LTE access, provided if available.
NOTE: Values not shown are not applicable to this standard.		

ELR Examples:

Initial ELR

```
<emerep ver="3.4.0">
  <eme_event eme_trigger="EME_ORG">
    <eme_pos>
      <msid>461011678298</msid>
      <servingcell>
        <mcc>234</mcc>
        <mnc>215</mnc>
        <lte_ci>546</lte_ci>
      </servingcell>
      <target_serving_node>
        <mme_name>mme1.operatorname.pub.3gppnetwork.org</mme_name>
      </target_serving_node>
    </eme_pos>
  </eme_event>
</emerep>
```

Handover ELR (from MME to MME)

```
<emerep ver="3.4.0">
  <eme_event eme_trigger="EME_HO">
    <eme_pos>
      <msid>461011678298</msid>
      <target_serving_node>
        <mme_name>mme1.operatorname.pub.3gppnetwork.org</mme_name>
      </target_serving_node>

    </eme_pos>
  </eme_event>
</emerep>
```

Handover ELR (from MME to VMSCID)

```
<emerep ver="3.4.0">
  <eme_event eme_trigger="EME_HO">
    <eme_pos>
      <msid>461011678298</msid>
```

```
      <msid type="IMEI">35850604062684</msid>
      <target_serving_node>
        <vmscid>
          <vmscno>1541154871</vmscno>
        </vmscid>
      </target_serving_node>
    </eme_pos>
  </eme_event>
</emerep>
```

Termination ELR

```
<emerep ver="3.4.0">
  <eme_event eme_trigger="EME_REL">
    <eme_pos>
      <msid>461011678298</msid>
    </eme_pos>
  </eme_event>
</emerep>
```

Annex C
(informative)

C Location Acquisition & Conveyance

This annex describes procedures applicable to location acquisition and conveyance to assist call routing and to provide location to the PSAP. These procedures correspond to procedures defined in 3GPP TS 23.271 [Ref 5] and OMA SUPL [Ref 11]. The procedures are considered informative in this standard because they copy portions of other standards.

C.1 Control Plane Location Solution

This subclause describes use of the control plane location solution as defined in 3GPP TS 23.271 [Ref 5] to obtain location for IMS emergency call origination (e.g., for routing) and subsequently while an emergency call is established, to provide either an initial location or an updated location to the PSAP. The figures in this subclause show a GMLC as an example of an LS. While the figures show the GMLC and LRF within a single box, this standard views the LS and LRF as distinct functional elements that may either be physically separate or integrated.

C.1.1 Control Plane Location for IMS Call Origination for LTE Access

Figure C.1 shows the procedure to support location when an IMS emergency call is originated using an LTE access.

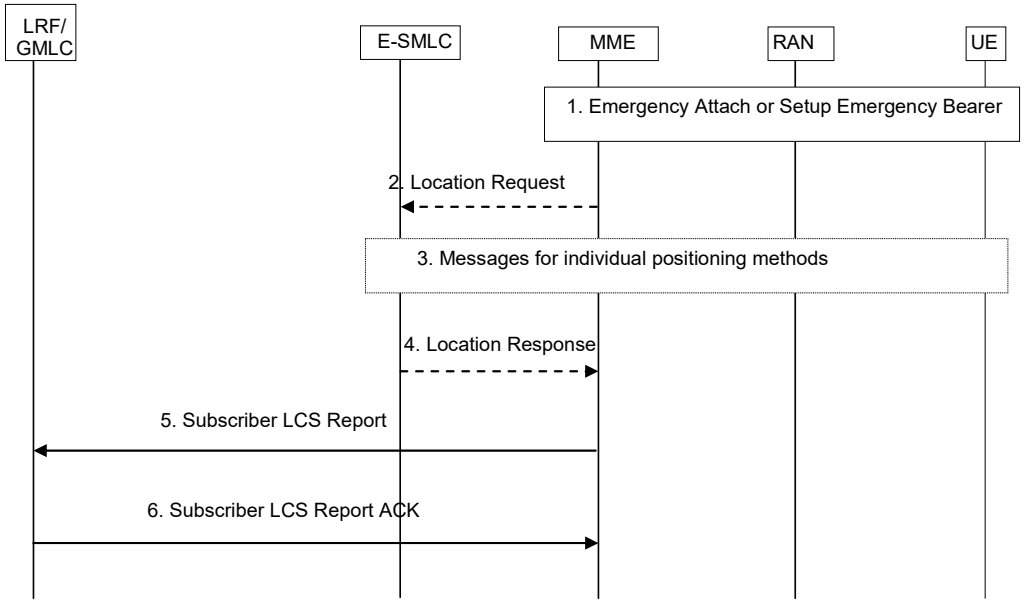

Figure C.1 – Control Plane Location for IMS Emergency Call Origination for LTE Access

Step 1. The user initiates an emergency call. The UE either performs an emergency attach if in limited service state or requests an emergency PDN connection if in normal service state and after performing a normal attach. Details of an emergency attach and normal attach for LTE can be found in 3GPP TS 23.401 [Ref 14].

Step 2. Steps 2 to 4 may be skipped if the MME only needs to send its identity or serving Cell ID to the LRF and not the location of the UE. Otherwise, the MME selects an E-SMLC and sends a Location Request message to the selected E-SMLC. The Location Request includes the type of location information requested, the requested QoS, identity of serving cell, and UE capability to support LPP. The requested QoS corresponds to that needed to obtain a location estimate sufficient to select a destination PSAP.

NOTE: If the UE was in connected mode prior to Step 1, the MME may not have the most current serving cell identity if there was an intra-eNodeB handover.

Step 3. If the requested location information and the location accuracy within the QoS can be satisfied based on parameters received from the MME (e.g., cell identity), the E-SMLC may send a Location Response immediately. Otherwise, the E-SMLC determines the positioning method and instigates the particular message sequence for this method as described in 3GPP TS 36.305 [Ref 20]. The positioning method may be either network centric or UE centric. If the position method or methods fail, the E-SMLC may use the current cell identity to derive an approximate location estimate.

Step 4. When a location estimate best satisfying the requested QoS has been obtained, the E-SMLC returns a Location Response to the MME with an indication whether the obtained location estimate satisfies the requested accuracy or not. This message carries the location estimate that was obtained. If a location estimate was not successfully obtained, a failure cause is included in the Location Response.

Step 5. The MME determines a GMLC using either the serving cell identity or some fixed association for the MME. The MME sends a Subscriber Location Report to the GMLC carrying the IMEI and if available the IMSI and MSISDN of the UE, the event causing the message (EPC NI-LR), and, if obtained in Steps 2 to 4, the location estimate. The serving cell identity of the UE needs to also be sent if available. The MME includes its own address.

Step 6. The GMLC returns an acknowledgment to the MME. The GMLC provides the received information to an associated LRF, which stores the information for future use. The LRF will use the information when later queried by an E-CSCF for routing information for the IMS emergency call which the UE will originate following Step 1. Since there is a possibility of the E-CSCF query being received by the LRF before the information is provided by the GMLC, the LRF may choose to wait a short period following the E-CSCF query for the GMLC provided information to become available. This treatment depends on consistent use by an operator of the control plane solution (e.g., use of the control plane solution for an entire LTE network).

C.1.2 Control Plane Location Subsequent to IMS Call Origination for LTE Access

Figure C.2 shows the procedure to obtain location after an IMS emergency call has been originated using an LTE access.

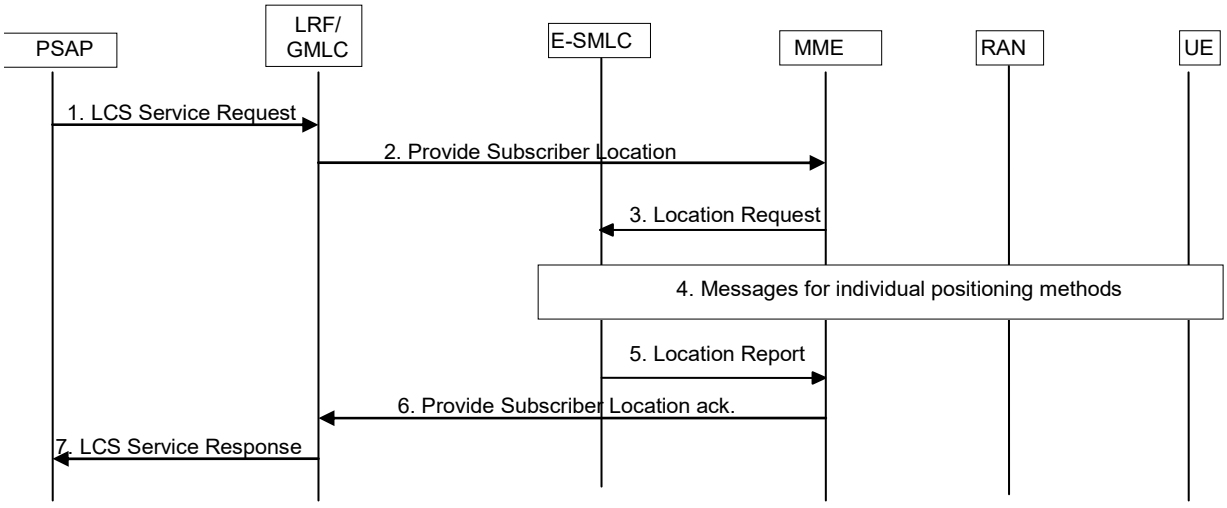

Figure C.2 – Control Plane Location following IMS Emergency Call Origination for LTE Access

Step 1. The LRF is identified using the location URI received in the SIP INVITE for the IMS Emergency Call Origination in the case of a PSAP accessed via a NENA i3 ESInet. For a PSAP accessed via a legacy emergency services network, the LRF is identified using either

the ESRK or ESRD received in the originating call request. The PSAP,NENA i3 ESInet, or legacy ALI system sends an LCS service request to the LRF. For a PSAP accessed via a legacy emergency services network, the ALI system will use either the Emergency Services Protocol (ESP) defined in ANSI J-STD-036-C-2 [Ref 7] or MLP defined by OMA [Ref 8]. For a PSAP accessed via a NENA i3 ESInet, the location URI will be an HTTP or HTTPS URI as defined in RFC 6442 [Ref 30] and the LCS Service Request will conform to the HELD dereferencing protocol defined in [Ref 9].

Step 2. The LRF determines the serving MME for the UE from information previously received via the GMLC either: (i) from the MME using the procedure described in Figure C.1 if there was no handover; or (ii) from the MME or some other serving node using the procedure described in Figure C.5 if handover has occurred. The LRF invokes an associated GMLC to send a Provide Subscriber Location message to the MME. The Provide Subscriber Location message carries, if available, the MSISDN or the IMSI and, if available, the IMEI for the target UE, as well as the required QoS and an indication of a location request from an emergency services client. The MME identifies the target UE using the IMSI, MSISDN, and/or the IMEI.

Step 3. The MME sends a Location Request to a selected E-SMLC and includes the QoS received in Step 2.

Step 4. The E-SMLC performs positioning as in Step 3 in Figure C.1.

Step 5. The E-SMLC returns a location estimate to the MME.

Step 6. The MME returns the location estimate to the LRF/GMLC. The information about the positioning method used may be sent with the location estimate.

Step 7. The LRF sends the location service response toward the PSAP.

C.1.3 Control Plane Location for IMS Call Origination for HSPA Access

Figure C.3 shows the procedure to obtain location when an IMS emergency call is originated using an HSPA access.

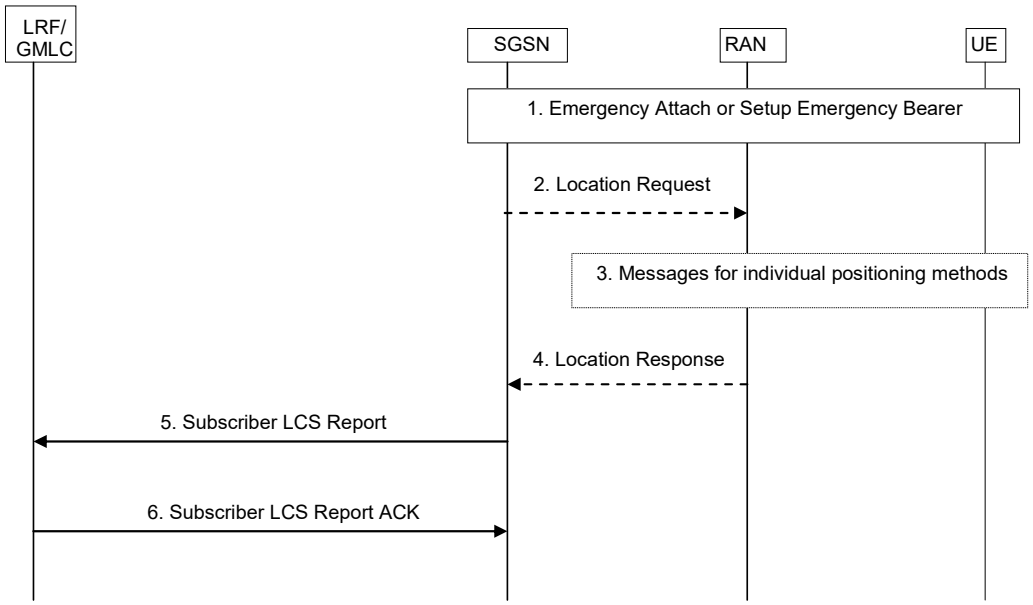

Figure C.3 – Control Plane Location for IMS Emergency Call Origination for HSPA Access

Step 1. The user initiated an emergency call. The UE either performs an emergency attach if in limited service state or requests an emergency PDP context if in normal service state and after performing a normal attach. Details of an emergency attach and normal attach for HSPA can be found in 3GPP TS 23.060 [Ref 23].

Step 2. Steps 2 to 4 may be skipped if the SGSN only needs to send its address to the LRF and not the location of the UE. Otherwise, the SGSN sends a Location Request message to the

serving RNC in the RAN. The Location Request includes the type of location information requested and the requested QoS. The requested QoS corresponds to that needed to obtain a location estimate sufficient to select a destination PSAP.

Step 3. If the requested location information and the location accuracy within the QoS can be satisfied based on parameters received from the SGSN and the parameters obtained by the RAN (e.g., cell coverage and timing information – i.e., RTT or Timing Advance), the RAN may send a Location Report immediately. Otherwise, the RAN determines the positioning method and instigates the particular message sequence for this method as described in 3GPP TS 25.305 [Ref 25]. The positioning method may be either network centric or UE centric. If the position method or methods fail, the RAN may use the current cell information and, if available, RTT or Timing Advance value to derive an approximate location estimate.

Step 4. When a location estimate best satisfying the requested QoS has been obtained, the RAN returns a Location Report to the SGSN with an indication whether the obtained location estimate satisfies the requested accuracy or not. This message carries the location estimate that was obtained. If a location estimate was not successfully obtained, a failure cause is included in the Location Report.

Step 5. The SGSN determines a GMLC using either the SAI or cell identity, or some fixed association for the SGSN. The SGSN sends a Subscriber Location Report to the GMLC carrying the IMEI and, if available, the IMSI and MSISDN of the UE, the event causing the message (PS NI LR), and, if obtained in Steps 2 to 4, the location estimate. The serving cell identity or SAI of the UE needs to also be sent if available. The SGSN includes its own address.

Step 6. The GMLC returns an acknowledgment to the SGSN. The GMLC provides the received information to an associated LRF, which stores the information for future use. The LRF will use the information when later queried by an E-CSCF for routing information for the IMS emergency call which the UE will originate following Step 1. Since there is a possibility of the E-CSCF query being received by the LRF before the information is provided by the GMLC, the LRF may choose to wait a short period following the E-CSCF query for the GMLC provided information to become available. This treatment depends on consistent use by an operator of the control plane solution (e.g., use of the control plane solution for an entire HSPA network).

C.1.4 Control Plane Location Subsequent to IMS Call Origination for HSPA Access

Figure C.4 shows the procedure to obtain location after an IMS emergency call has been originated using an HSPA access.

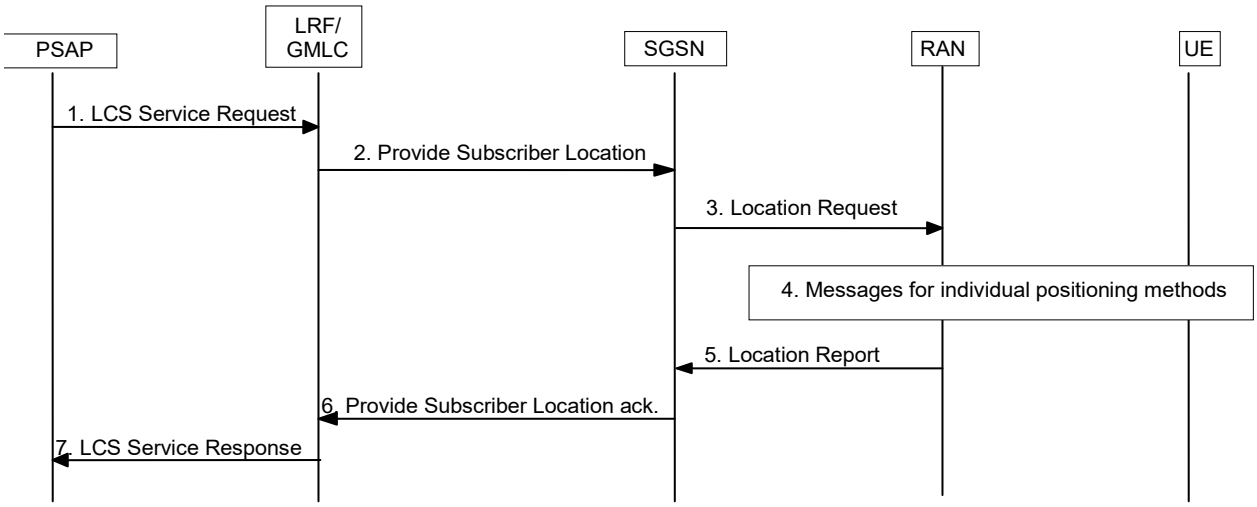

Figure C.4 – Control Location following IMS Emergency Call Origination for HSPA Access

Step 1. The LRF is identified using the location URI received in the SIP INVITE for the IMS Emergency Call Origination in the case of a PSAP accessed via a NENA i3 ESInet. For a PSAP accessed via a legacy emergency services network, the LRF is identified using either the ESRK or ESRD received in the originating call request. The PSAP, NENA i3, or legacy ALI system ESInet sends an LCS service request to the LRF. For a PSAP accessed via a legacy emergency services network, the ALI system will use either the Emergency Services Protocol (ESP) defined in ANSI J-STD-036-C-2 [Ref 7] or MLP defined by OMA [Ref 8]. For a PSAP accessed via a NENA i3 ESInet, the location URI will be an HTTP or HTTPS URI as defined in RFC 6442 [Ref 30] and the LCS Service Request will conform to the HELD dereferencing protocol defined in [Ref 9].

Step 2. The LRF determines the serving SGSN for the UE from information previously received either: (i) from the SGSN using the procedure described in Figure C.3 if there was no handover; or (ii) from the SGSN or some other serving node using the procedure described in Figure C.5 if handover has occurred. The LRF invokes an associated GMLC to send a Provide Subscriber Location message to the SGSN. The Provide Subscriber Location message carries, if available, the MSISDN or the IMSI and, if available, the IMEI for the target UE, as well as the required QoS and an indication of a location request from an emergency services client. The GMLC identifies the target UE using the IMSI, MSISDN, and/or the IMEI.

Step 3. The SGSN sends a Location Request to the serving RNC in the RAN and includes the QoS received in Step 2.

Step 4. The RAN performs positioning as in Step 3 in Figure C.3.

Step 5. The RAN returns a location estimate to the SGSN.

Step 6. The SGSN returns the location estimate to the LRF/GMLC. The information about the positioning method used may be sent with the location estimate.

Step 7. The LRF sends the location service response toward the PSAP.

C.1.5 Location Continuity following handover of an IMS Emergency Call

Figure C.5 shows the procedure used to update the LRF with the identity of a new target serving node following handover of an IMS emergency call from some source node to a target node. The procedure allows for the possibility that the source and target nodes may be associated with different GMLCs (provided both GMLCs are associated with the same LRF). The procedure is valid for the following combinations of source and target access types and corresponding nodes.

Source Access (Node): LTE (MME) or HSPA (SGSN)

Target Access (Node): LTE (MME), HSPA (SGSN), GERAN or UTRAN in the CS domain (MSC server), 1x RTT (MSC – note 1), eHRPD (note 2)

NOTE 1: This is applicable only for LTE access on the source side.

NOTE 2: There is no target node for eHRPD.

The procedure may be used with a control plane location solution on one side (source or target) and a user plane solution on the other side, or with a control plane solution on both sides. The procedure is not needed when a user plane location solution is used on both sides.

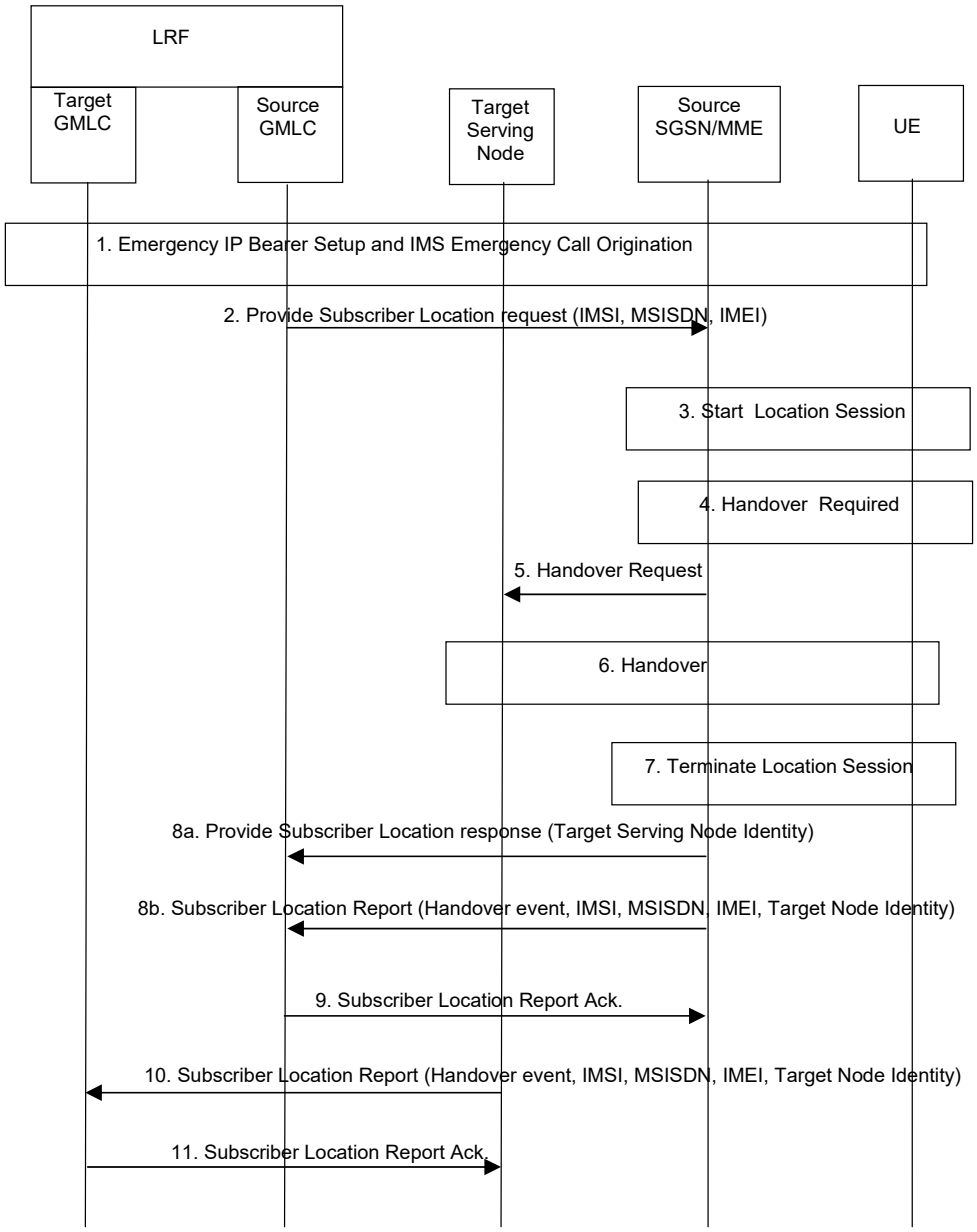

Figure C.5 – Location Continuity following handover of an IMS Emergency Call

Step 1. The UE establishes an IMS emergency call and, if the control plane location solution is used on the source side, the serving MME or SGSN may execute the procedure in Figure C.1 or Figure C.3, respectively, to obtain an initial location estimate and provide the LRF with both the location estimate and its own address.

Step 2. At some later time, if the control plane location solution is used on the source side, the serving MME or SGSN may receive a request from a GMLC associated with the LRF (hereafter referred to as the source GMLC) for the location of the UE according to the procedure in Figure C.2 or Figure C.4, respectively.

Step 3. If Step 2 occurs, the source MME or SGSN starts a location session to obtain the location of the UE. Note that a location session could instead be instigated as part of Figure C.1 or Figure C.3 if handover occurs before the MME or SGSN is able to provide the initial location estimate and its own address to the LRF in Step 1.

Step 4. A request is later sent to the source MME from the serving eNodeB (for LTE access) or to the source SGSN from the serving RNC (for HSPA access) for a handover to a particular target eNodeB (for handover to LTE) or target RNC (for handover to HSPA) or target MSC

server (for handover to UTRAN CS or GERAN CS) or target cell associated with a particular 1xRTT MSC (for handover to 1xRTT) or HRPD target cell (for handover to HRPD).

Step 5. For handover to LTE, HSPA, UTRAN CS, or GERAN CS, the source MME or SGSN sends a Handover Request message to the target MME, SGSN, MSC server, or MSC server (hereafter referred to as the target serving node) in each case respectively as defined in 3GPP TS 23.401 [Ref 14], TS 23.060 [Ref 23], or TS 23.216 [Ref 19]. For handover from LTE to 1xRTT, the source MME initiates a handover to a target 1xRTT IWS using single radio voice call continuity procedures as described in 3GPP TS 23.216 [Ref 19]. For handover from LTE to HRPD, this step does not occur.

Step 6. The rest of the handover preparation and execution procedure is completed as defined in 3GPP TS 23.401 [Ref 14], TS 23.402 [Ref 15], TS 23.060 [Ref 23], or TS 23.216 [Ref 19].

Step 7. Any location session started in Step 3 may terminate normally before Step 6 is complete. If not, the source SGSN or MME aborts the session once Step 6 is complete. This may lead to provision of a location estimate for the UE to the source SGSN or MME.

Step 8. a) If the control plane location solution is used on the source side and Step 2 occurred, the source SGSN or MME returns a Provide Subscriber Location response to the source GMLC carrying any location estimate obtained for the UE in Step 3. Depending on configuration information in the source SGSN or MME (e.g., which may be related to the source and target serving node identities, the location capabilities of the UE and whether the UE is roaming or not), the Provide Subscriber Location response may – except for handover to HRPD – convey the identity of the target serving node.

b) If the control plane location solution is used on the source side but Steps 2 and 8a do not occur, the source SGSN or MME may – depending on configuration information in the source SGSN or MME (e.g., as in Step 8a) – send a Subscriber Location Report to the source GMLC carrying the UE identity (IMSI, MSISDN, and/or IMEI), an event type indicating handover and – except for handover to HRPD – the identity of the target serving node.

Step 9. The source GMLC acknowledges the message in Step 8b if this occurs.

Step 10. Steps 10 and 11 only apply when the target side supports a 3GPP access type (e.g., does not apply to 1xRTT or HRPD) and are only needed when the identity of the target node is not provided by the source node in Step 8a or 8b. Note that knowledge of whether Step 8a or 8b was performed would have to be configured – i.e., an operator would need to consistently use either Steps 8a/8b or Step 10. Depending on configuration information in the target serving node (e.g., which may be related to the source and target serving node identities, the location capabilities of the UE, and whether the UE is roaming or not), the target serving node may after handover in Step 6 is complete send a Subscriber Location Report to a GMLC on the target side if the control plane location solution will be used on the target side. The Subscriber Location Report carries the UE identity (IMSI, MSISDN and/or IMEI), an event type indicating handover and the identity of the target serving node. However, no location estimate is included. The target serving node may determine the address of the target GMLC from configuration information.

Step 11. The target GMLC acknowledges the message in Step 10. The information obtained by the target GMLC in this step or by the source GMLC in Step 8a or Step 8b is provided to the LRF. The LRF may use this information to support future location requests from a PSAP to the UE as described in Figure C.2, Figure C.4, and Figure C.7.

C.2 User Plane Location Solution

This subclause describes use of the user plane location solution defined in OMA SUPL [Ref 11] to obtain location on initial IMS emergency call origination (e.g., for routing), and subsequently while an emergency call is established to provide either an initial accurate location or an updated location.

C.2.1 User Plane Location for IMS Call Origination

Figure C.6 shows the procedure to support user plane location when an IMS emergency call is originated if location is needed to select a destination PSAP. The procedure applies to LTE, HSPA, and HRPD access.

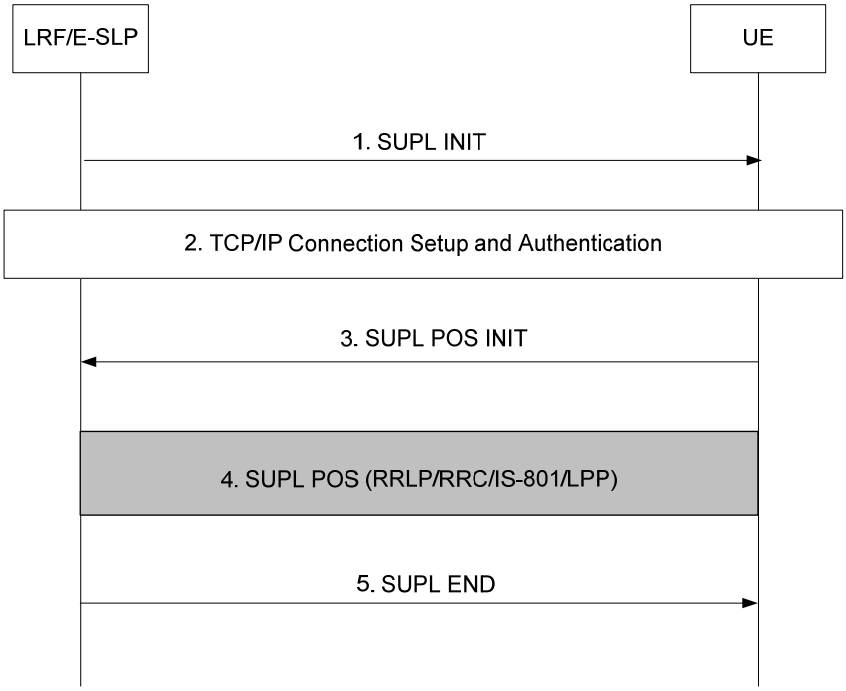

Figure C.6 – User Plane Location for IMS Emergency Call Origination for LTE, HSPA, and HRPD Access

Step 1. The LRF invokes an associated E-SLP to initiate a user plane location session with the UE. The E-SLP sends a SUPL INIT message to the UE. In North America, the SUPL INIT message needs to transfer using UDP/IP. The SUPL INIT contains at least a session-id, proxy mode indicator, and the intended positioning method. The SUPL INIT also contains the E-SLP address if the E-SLP is not known to be the H-SLP for the UE. The SUPL INIT may contain the desired QoS. The E-SLP also includes a Notification element in the SUPL INIT message indicating location for emergency services and an indication that notification or verification to the target SET is not required. Before the SUPL INIT message is sent, the E-SLP also computes and stores a hash of the message.

NOTE: In North America, Notification element in the SUPL INIT is required. The user is not notified and not allowed to accept or reject the location request.

Step 2. The UE establishes a TCP/IP connection to the E-SLP using either the E-SLP address provided in Step 1 or the H-SLP address configured in the UE if no E-SLP address was provided in Step 1. The E-SLP and the UE then perform authentication – minimally the UE authenticates the E-SLP and the E-SLP may authenticate the UE as described in OMA-TS-ULP-V2_0 [Ref 11].

Step 3. The UE sends a SUPL POS INIT message to start a positioning session with the E-SLP. The SUPL POS INIT message contains at least the session-id, SET capabilities, a hash of the received SUPL INIT message, and Location ID. The SET capabilities include the supported positioning methods and associated positioning protocols (e.g., RRLP, RRC, IS-801, or LPP). The SET may provide network radio measurements specific for the access being used in the Location ID parameter. The SET may provide its position, if this is available. The UE may include a request for assistance data in the case of LTE or HSPA access.

Step 4. The E-SLP verifies that the hash of the SUPL INIT matches the one it has computed for this particular session. If a position estimate was included in Step 3 of sufficient accuracy, the E-SLP may proceed to Step 5. Otherwise, based on the SUPL POS INIT message including position methods supported by the UE, the E-SLP determines the position method and instigates a positioning session with the UE in which SUPL POS messages are exchanged carrying positioning messages according to one of the positioning protocols supported by the UE – either RRLP, RRC, IS-801, or LPP. The positioning procedure will terminate when the E-SLP receives from the UE sufficient measurements to compute a

location estimate satisfying the required QoS or a location estimate satisfying the QoS computed by the UE.

Step 5. Once the position session is complete, the E-SLP sends a SUPL END message to the UE to terminate the location session. The UE releases the TCP/IP connection to the E-SLP and releases all resources related to this session. The E-SLP transfers the location estimate to the LRF.

C.2.2 User Plane Location Subsequent to IMS Call Origination

Figure C.7 shows the procedure to obtain location with a user plane location solution after an IMS emergency call has been originated. The procedure applies to LTE, HSPA, and HRPD access.

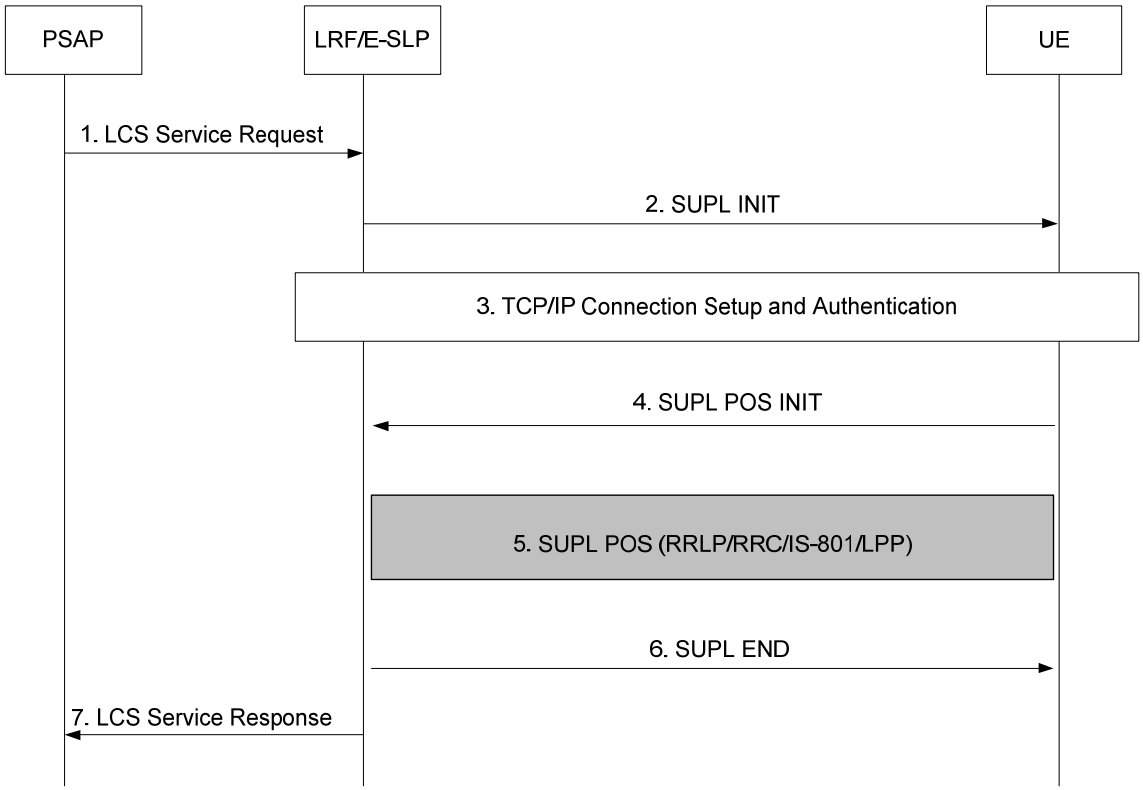

Figure C.7 – User Plane Location following IMS Emergency Call Origination for LTE, HSPA, and HRPD Access

Step 1. The LRF is identified using the location URI received in the SIP INVITE for the IMS Emergency Call Origination in the case of a PSAP accessed via a NENA i3 ESInet. For a PSAP accessed via a legacy emergency services network, the LRF is identified using either the ESRK or ESRD received in the originating call request. The PSAP, NENA i3, or legacy ALI system ESInet sends an LCS service request to the LRF. For a PSAP accessed via a legacy emergency services network, the ALI system will use either the Emergency Services Protocol (ESP) defined in ANSI J-STD-036-C-2 [Ref 7] or MLP defined by OMA [Ref 8]. For a PSAP accessed via a NENA i3 ESInet, the location URI will be an HTTP or HTTPS URI as defined in RFC 6442 [Ref 30] and the LCS Service Request will conform to the HELD dereferencing protocol defined in [Ref 9].

Step 2. **to Step 6**. These steps are the same as Steps 1 to 5 for Figure C.6, except that the QoS included in the SUPL INIT by the E-SLP in Step 2 will correspond to the location accuracy needed for the PSAP.

Step 7. The LRF sends the location service response toward the PSAP.

Annex D
(informative)

D Routing Methodology

The routing methodology described in this annex allows various types of emergency calls that might be originated by IMS subscribers to be routed to the appropriate ESInet or legacy emergency services network in a way that is optimized for the interconnected emergency services network. See Figure D.1 through Figure D.7 for flow charts that illustrate the routing methodology described in this annex.

This standard assumes that when an emergency call/session is initiated by the UE, it will be sent to a P-CSCF. The P-CSCF will then forward the emergency call/session request to an E-CSCF, which will, in turn, forward the request to the LRF to obtain location and/or routing information for that call/session.

UE location information is needed to help drive the routing mechanism provided by the RDF component of the LRF. If a location value has been provided in the session request from the E-CSCF, the LRF need not invoke location retrieval functionality prior to invoking routing determination functionality. If UE location is not available in the session request forwarded by the E-CSCF, the LRF will use a location acquisition technique that is appropriate for the call type. For example:

- If the session request received by the LRF contains a “telephone number” (and no location-by-value or location-by-reference), the LRF will consult with an appropriate Location Server (LS) for the call type (i.e., based on the content of the P-Access-Network-Info header) to obtain location information associated with the call (e.g., an LS that contains pre-provisioned mappings from telephone numbers to fixed locations).
- If the session request received by the LRF contains MSISDN/MDN and cell site information, the LRF will consult with an appropriate LS (e.g., a GMLC) to initiate location determination. (Note that it is expected that cell-based location information will be used in the initial routing of the call.)
- If the session request received by the LRF contains a location reference URI, the LRF will de-reference that location reference URI (i.e., send a de-reference request to the entity identified by the location reference URI) to obtain a location-by-value for the call.

Having obtained a location value for the call, the LRF will interact with the RDF, using the location information as input to the route determination process (e.g., using the LoST protocol to interact with an external RDF). The RDF will return routing information (e.g., a Route URI) that will cause the call to be directed either toward a NENA i3 ESInet or toward a legacy emergency services network.

Based on the information that the LRF received from the E-CSCF with the emergency call/session request and the emergency services network toward which the emergency call/session is to be directed, the LRF will determine:

- Whether a Reference Identifier (e.g., a 10-digit number in the form of a URI, or a location URI) needs be associated with the call.
- What information should be returned to the E-CSCF.

If the call is destined for a legacy emergency services network, a Reference Identifier (in the form of 10-digit number) allocated by the LRF and/or a callback number will need to be provided to the legacy emergency services network with the call. The LRF will either return a Reference Identifier and a routing URI, possibly along with a callback number, to the E-CSCF, or it may return just a routing URI (for the case where the telephone number received with the emergency call/session request is to be forwarded by the E-CSCF).

If the call is destined for a NENA i3 ESInet, the original call/session request contained a telephone number, and the LRF, through its interactions with an LS, identified static location information associated with the call, the LRF will not associate a Reference Identifier with the call. Instead, the LRF will return the static location (as a location-by-value) to the E-CSCF, along with the routing URI. The E-CSCF should send the call/session request forward to the ESInet with the routing URI, the location-by-value, and whatever callback information was received with the original emergency call/session request.

If the call is destined for a NENA i3 ESInet and a routing location based on cell-related information was used by the RDF in routing the call, the LRF will allocate a Reference Identifier (e.g., a location URI) to the call and return the Reference Identifier and the routing URI to the E-CSCF. The E-CSCF will send the call/session request forward to

the ESInet with the routing URI, the Reference Identifier allocated by the LRF, and whatever callback information was received with the original emergency call/session request.

If the call is destined for a NENA i3 ESInet, and the original call/session request contained a location reference URI, the LRF will first de-reference the location reference URI to obtain the associated location-by-value, then use that location-by-value to interact with the RDF for routing information. The LRF will not associate a Reference Identifier with the call, but will return the Route URI and, optionally, the location reference URI and whatever callback information it received in the original call/session request, back to the E-CSCF. The E-CSCF will send the emergency call/session request forward to the ESInet with the routing URI, the location reference URI and the callback information.

If an E-CSCF receives a SIP INVITE message associated with an emergency session request, and no P-Asserted-Identity header field is present (i.e., because the emergency call/session request is originated by a mobile device/UE that does not have a valid callback number associated with it), then the E-CSCF shall insert a P-Asserted-Identity header field set to a non-dialable callback number (as defined in 3GPP TS 24.229 [Ref 2]) in the SIP INVITE message it sends to the LRF. If the call is destined for a NENA i3 ESInet, the non-dialable callback number will be sent to the NENA i3 ESInet as callback information. If the call is destined for a legacy emergency services network, and the legacy SR expects both a Reference Identifier and callback information, the non-dialable callback number will be forwarded to the legacy Emergency Services Network via the MGCF/MGW. If the call is destined for a legacy emergency services network, and the legacy SR expects to receive only a Reference Identifier, then the non-dialable callback number will not be forwarded to the legacy emergency services network via the MGCF/MGW. (It will, however, be returned by the LRF to the ALI system in an E2 esposreq message.)

D.1 Flow Charts for Routing Methodology

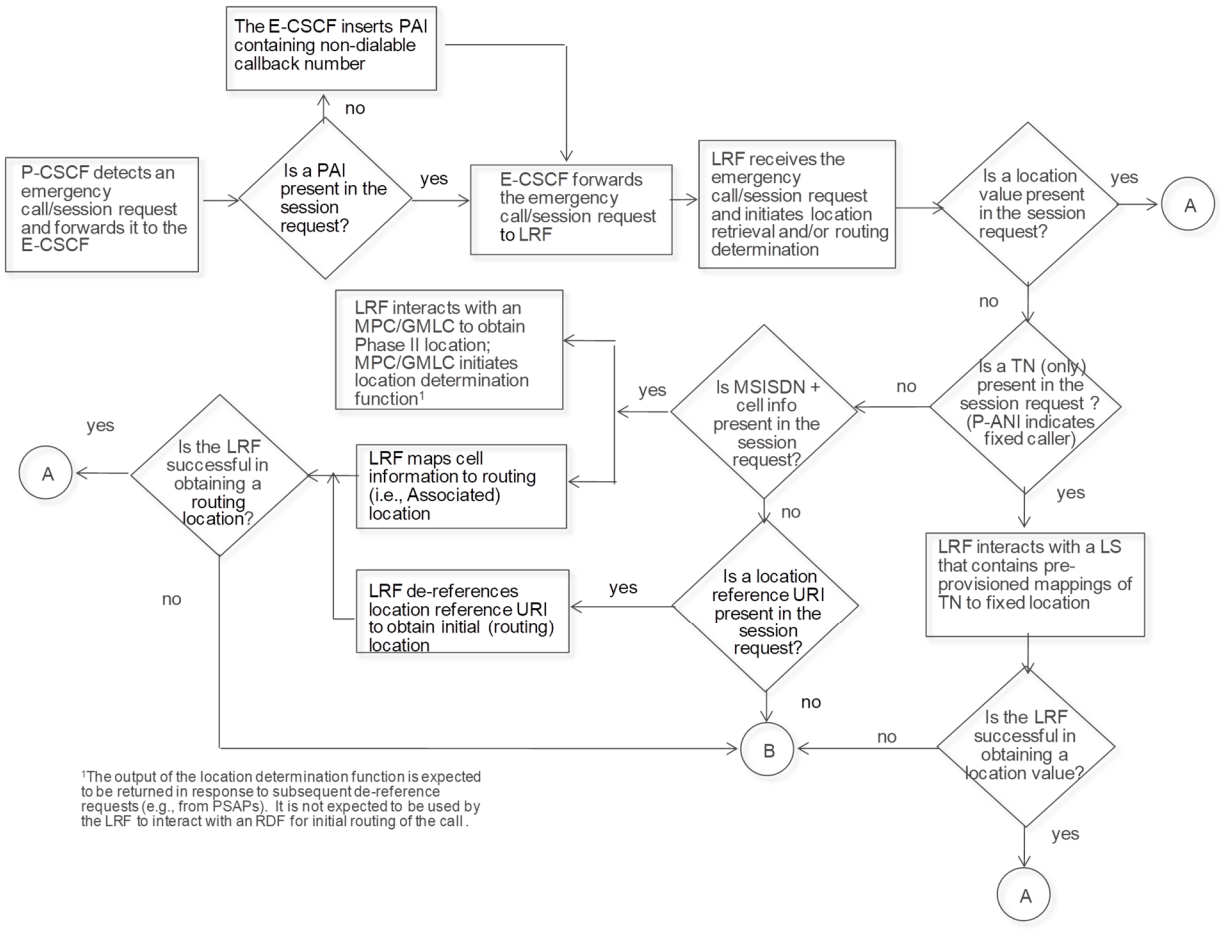

Figure D.1 – Emergency Call is Detected by IMS Origination Network and Routing Location is Acquired/Derived

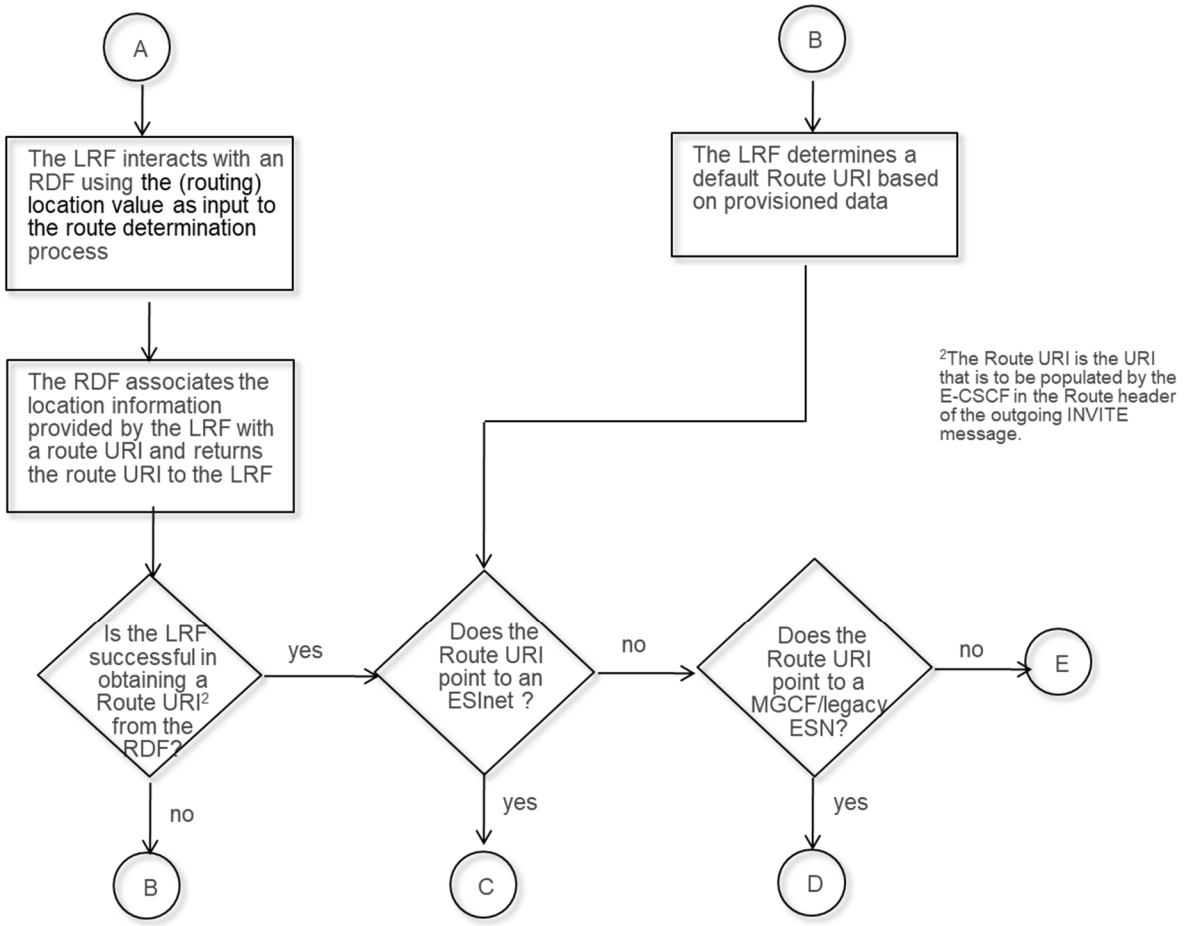

Figure D.2 – Route URI is Determined

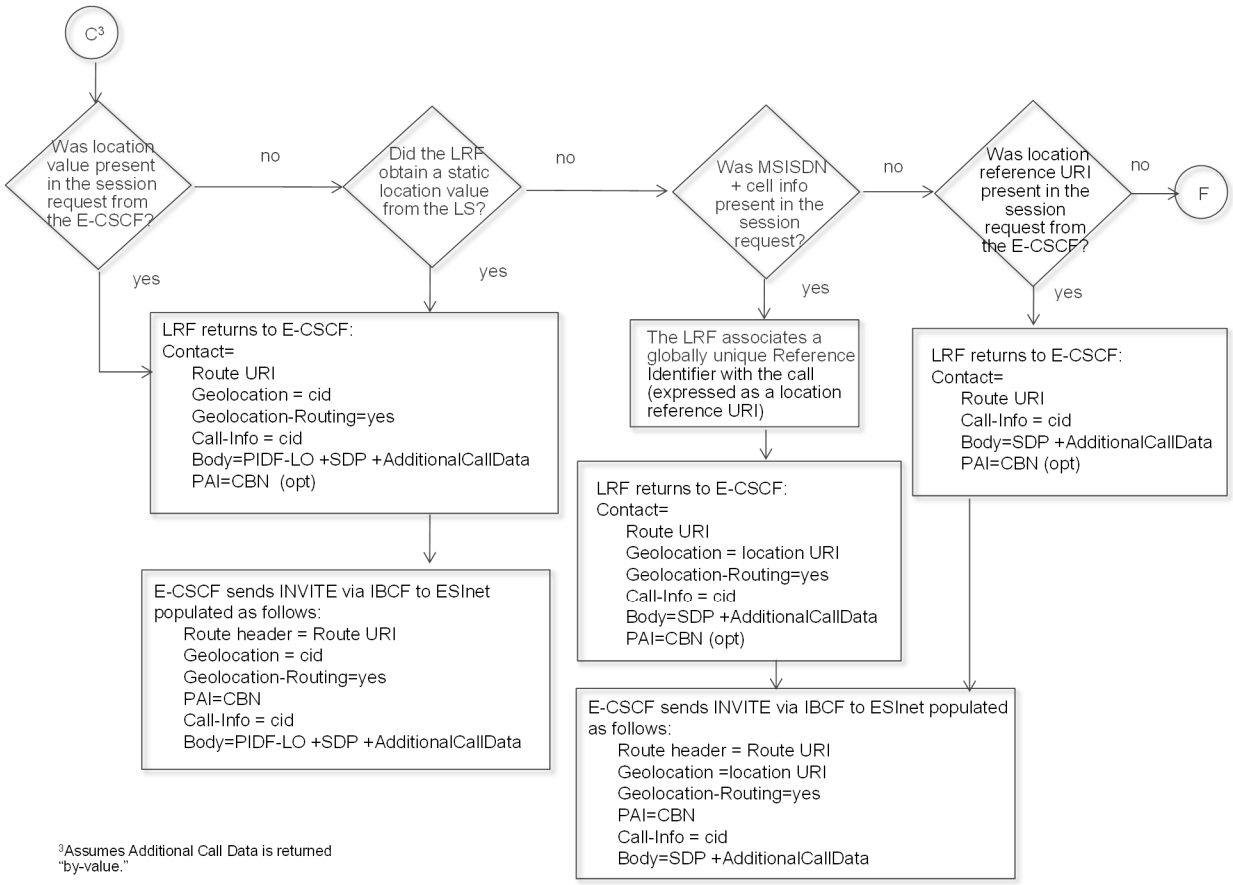

Figure D.3 – Emergency Call is Routed to NENA i3 ESInet – Additional Data "By-Value"

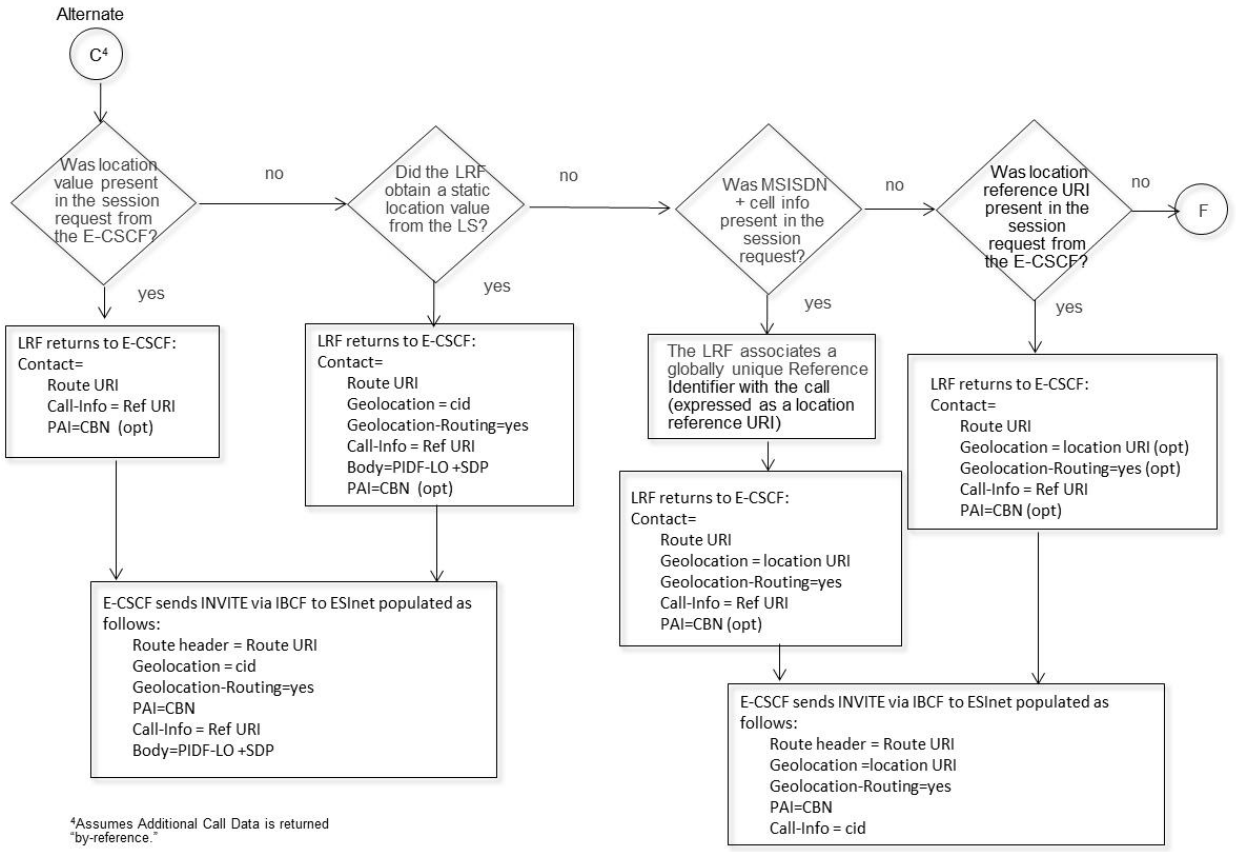

Figure D.4 – Emergency Call is Routed to NENA i3 ESInet – Additional Data "By-Reference"

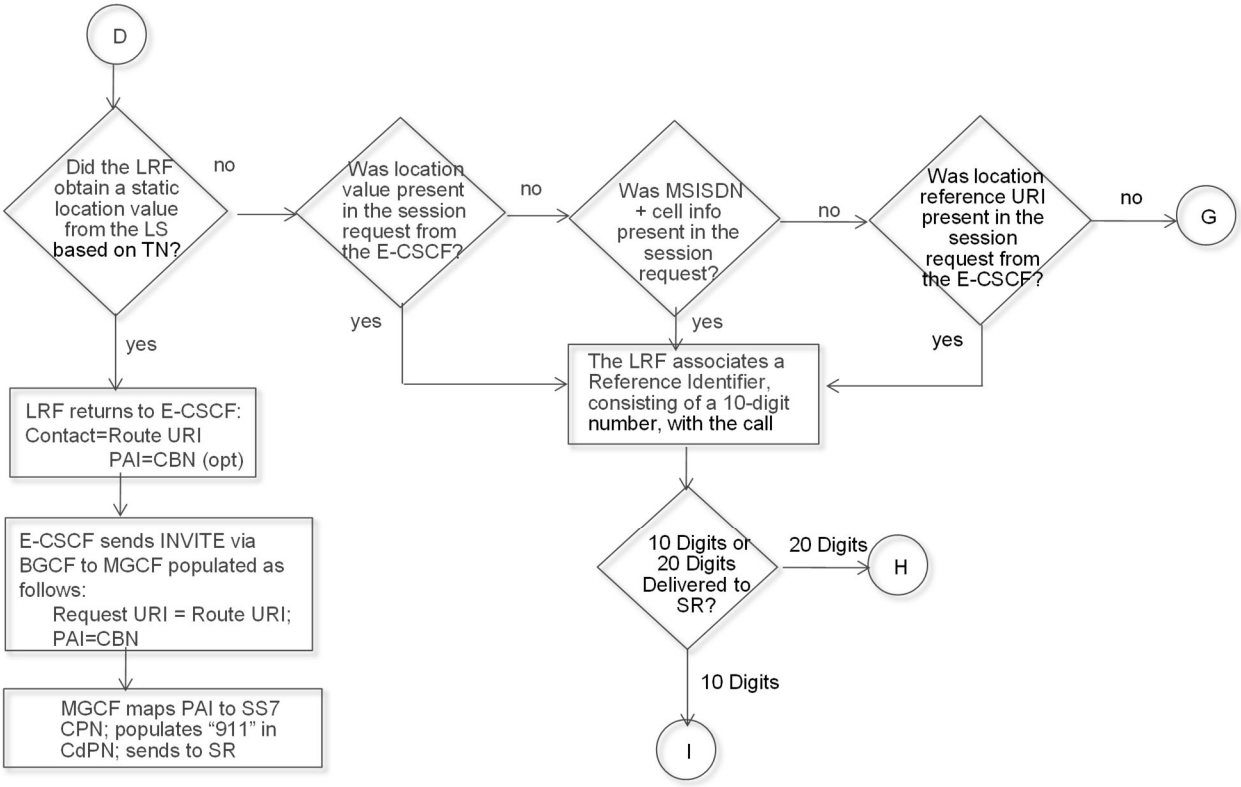

Figure D.5 – LRF Determines that Emergency Call is to be Routed to Legacy Emergency Services Network

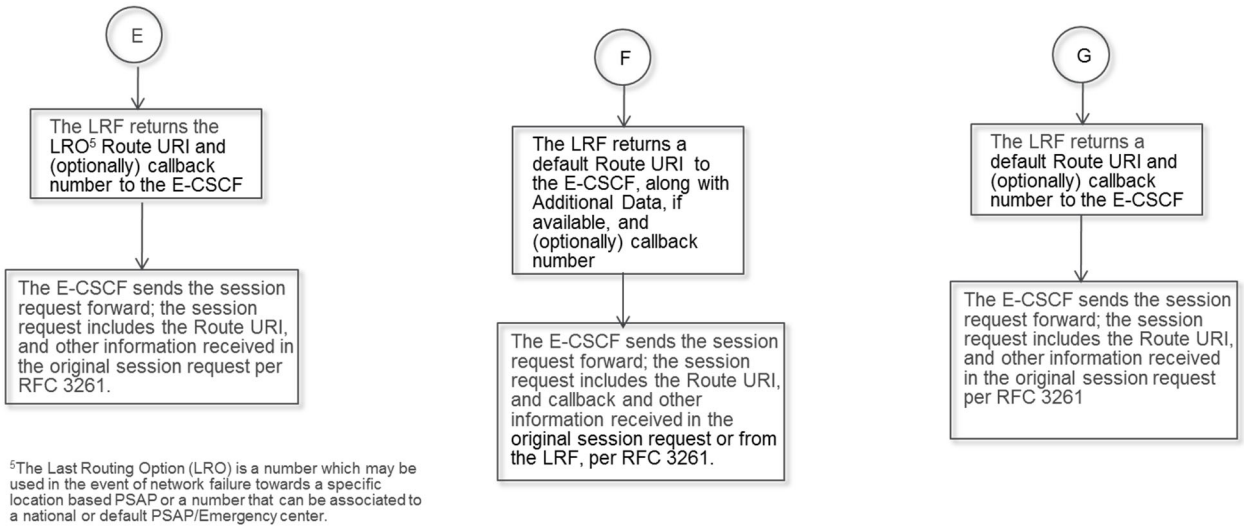

Figure D.6 – Emergency Call is Routed via Default or LRO Route URI

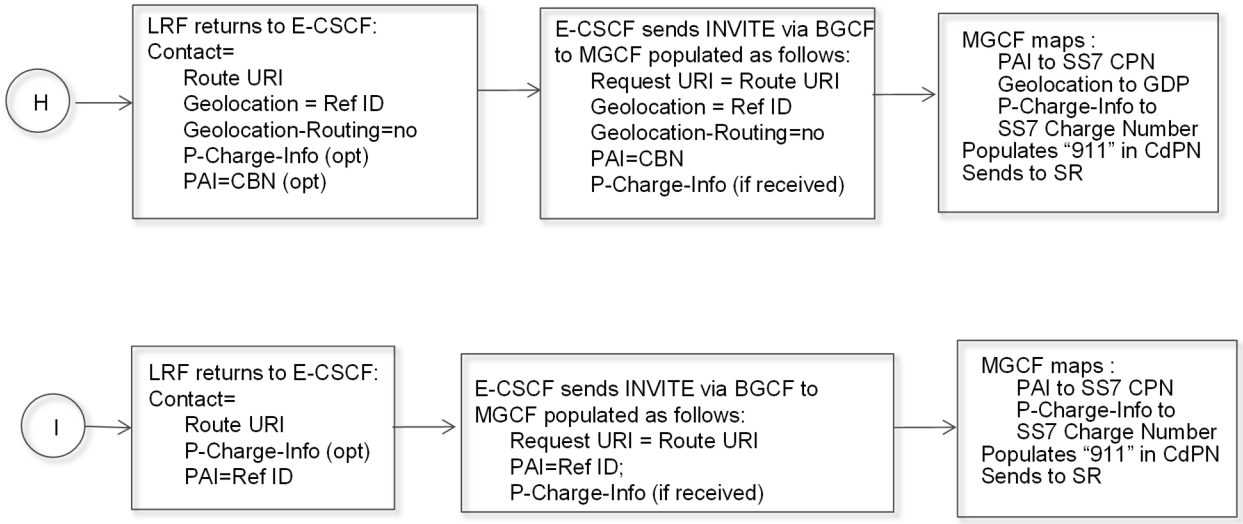

Figure D.7 – Emergency Call is Delivered to Legacy SR with 10 or 20 Digits of Information

Annex E
(informative)

E Message Examples

This informative annex provides message examples for various use cases.

E.1 SIP INVITE Sent from P-CSCF to E-CSCF for Fixed-line UE

The following represents an example of a SIP INVITE sent from P-CSCF to E-CSCF for an emergency call originated from a fixed-line UE. Note not all headers are shown:

```
INVITE urn:service:sos SIP/2.0
Via: SIP/2.0/UDP p-cscf.carrier.example.net;branch=z9hG4bK776asdhds
Via: SIP/2.0/UDP ue.carrier.example.net;branch= z9hG4bK813ar6k
Route: <sip:e-cscf.carrier.example.net;lr>
Record-Route: <sip:p-cscf.carrier.example.net;lr>
From: <sip:+13125551234@carrier.example.net;user=phone>;tag=23ac
To: <urn:service:sos>
Contact: <sip:+13125551234@carrier.example.net;user=phone>
P-Asserted-Identity: <sip:+13125551234@carrier.example.net;user=phone>
Max-Forwards: 69
Call-ID: 19dn30
CSeq: 1 INVITE
Supported: 100rel
Content-Type: application/sdp
Content-Length: nn
[SDP here]
```

E.2 SIP INVITE Sent from E-CSCF to LRF for Fixed-line UE

The following represents an example of a SIP INVITE sent from E-CSCF to LRF for an emergency call originated from fixed-line UE where a Reference Identifier that is different from the callback number is created by the LRF:

```
INVITE urn:service:sos SIP/2.0
Via: SIP/2.0/UDP e-cscf.carrier.example.net;branch= z9hG4bKbk46531a
Via: SIP/2.0/UDP p-cscf.carrier.example.net;branch=z9hG4bK776asdhds
Via: SIP/2.0/UDP ue.carrier.example.net; branch=z9hG4bK93cke34014
Route: <sip:lrf.lrfprovider.net;lr>
From: <sip:+13125551234@carrier.example.net;user=phone>;tag=23ac
To: <urn:service:sos>
Contact: <sip:+13125551234@carrier.example.net;user=phone>
P-Asserted-Identity: <sip:+13125551234@carrier.example.net;user=phone>
P-Charging-Vector: icid=34c23c445902;
 icid-generated-at=e-cscf.carrier.example.net;orig-ioi="Type 3
carrier.example.net"
Max-Forwards: 68
Call-ID: 19dn30
CSeq: 1 INVITE
Supported: 100rel
Content-Type: application/sdp
Content-Length: nn
[SDP here]
```

E.3 SIP INVITE Sent from E-CSCF towards the Legacy PSAP for Fixed-line UE

The following represents an example of a SIP INVITE sent from E-CSCF towards the legacy PSAP for an emergency call originated from fixed-line UE:

```
INVITE sip:+17735554321@carrier.example.net;user=phone SIP/2.0
Via: SIP/2.0/UDP e-cscf.carrier.example.net;branch=z9hG4bK9j1ck4kh
Via: SIP/2.0/UDP p-cscf.carrier.example.net;branch=z9hG4bK776asdhds
Via: SIP/2.0/UDP ue.carrier.example.net; branch=z9hG4bK93cke34014
From: <sip:+13125551234@carrier.example.net;user=phone>;tag=23ac
To: <urn:service:sos>
Contact: <sip:+13125551234@carrier.example.net;user=phone>
P-Asserted-Identity: <sip:+13125551234;
cpc=emergency;oli=00@carrier.example.net;user=phonea> #Reference Identifier
P-Charging-Vector: icid=34c23c445902;
 icid-generated-at=e-cscf.carrier.example.net;orig-ioi=carrier.example.net
Route: <sip:bgcf.carrier.example.net;lr>
Record-Route: <sip:e-cscf.carrier.example.net;lr>
Record-Route: <sip:p-cscf.carrier.example.net;lr>
Max-Forwards: 67
Call-ID: 19dn30
CSeq: 1 INVITE
Supported: 100rel
Content-Type: application/sdp
Content-Length: nn
[SDP here]
```

E.4 Response from the LRF to the E-CSCF for a Call that is to be Routed to a Legacy Emergency Services Network

This example illustrates a response from the LRF to the E-CSCF for a call that is to be routed to a legacy emergency services network.

```
SIP/2.0 300 Multiple Choices
Via: SIP/2.0/UDP e-cscf.carrier.example.net;branch=z9hG4bKk9eb5810k
Via: SIP/2.0/UDP p-cscf.carrier.example.net;branch=z9hG4bK776asdhds
Via: SIP/2.0/UDP ue.carrier.example.net; branch=z9hG4bKdko0w45gks
From: <sip:+13125551234@carrier.example.net;user=phone>;tag=23ac
To: <urn:service:sos>
Call-ID: 19dn30
CSeq: 1 INVITE
Contact:<sip:+17735554321@carrier.example.net;user=phone?P-Asserted-
Identity=sip:+13125551234;cpc=emergency;oli=00@carrier.example.net;user=phone
>
P-Charging-Vector: icid=869a5e5214b;
 icid-generated-at=lrf.lrfprovider.net;orig-ioi=lrfprovider.net; orig-
ioi="Type 3 carrier.example.net"; term-ioi="Type 3 lrf.example.net"
Content-Length: 0
```

NOTE: The above Contact header field example is presented for readability. The actual syntax requires that reserved characters be escaped. The following is the resulting syntax:

Contact: < sip:+17735554321@carrier.example.net;user=phone?P-Asserted-Identity=sip:+13125551234%3Bcpc%3Demergency%3Boli%3D00%40carrier.example.net%3Buser%3Dphone >

E.5 Response from the LRF to the E-CSCF for a Call that is to be Routed to an ESInet

This example illustrates a response from the LRF to the E-CSCF for a call that is to be routed to an ESInet.

E.5.1 Response from LRF Containing Location-by-Reference

```
SIP/2.0 300 Multiple Choices
Via: SIP/2.0/UDP e-cscf.carrier.example.net;branch=z9hG4bK9kwu02kcew
Via: SIP/2.0/UDP p-cscf.carrier.example.net;branch=z9hG4bK776asdhds
Via: SIP/2.0/UDP ue.carrier.example.net; branch=z9hG4bKk0v471ckty
From: <sip:+13125551234@carrier.example.net;user=phone>;tag=23ac
To: <urn:service:sos>
Call-ID: 19dn30
CSeq: 1 INVITE
Contact: <sip:esrp.esinet.net?Geolocation-Routing=yes&
 Geolocation=<http://lrf.lrfprovider.net/9xkei90z>>
P-Charging-Vector: icid=869a5e5214b;
 icid-generated-at=lrf.lrfprovider.net; orig-ioi="Type 3 carrier.example.net";
term-ioi="Type 3 lrf.example.net"
```

NOTE: The above Contact header field example is presented for readability. The actual syntax requires that reserved characters be escaped. The following is the resulting syntax:

Contact:
< sip:esrp.esinet.net?Geolocation-Routing=yes&Geolocation= %3Chttp://lrf.lrfprovider.net/9xkei90z%3E >

E.5.2 Response from LRF Containing Location-by-Value

```
SIP/2.0 300 Multiple Choices
Via: SIP/2.0/UDP e-cscf.carrier.example.net;branch=z9hG4bK9kwu02kcew
Via: SIP/2.0/UDP p-cscf.carrier.example.net;branch=z9hG4bK776asdhds
Via: SIP/2.0/UDP ue.carrier.example.net; branch=z9hG4bKk0v471ckty
From: <sip:+13125551234@carrier.example.net;user=phone>;tag=23ac
To: <urn:service:sos>
Call-ID: 19dn30
CSeq: 1 INVITE
Contact: <sip:esrp.esinet.net?Geolocation-Routing=yes&
 Geolocation=<cid:target123@someoperator.example.com>>
P-Charging-Vector: icid=869a5e5214b;
  icid-generated-at=lrf.lrfprovider.net; orig-ioi="Type 3
carrier.example.net"; term-ioi="Type 3 lrf.example.net"
Content-Type= multipart/mixed
body=
[SDP and PIDF-LO here]
```

NOTE: The above Contact header field example is presented for readability. The actual syntax requires that reserved characters be escaped. The following is the resulting syntax:

Contact: < sip:esrp.esinet.net?Geolocation-Routing=yes&Geolocation=
%3Ccid:target123%40someoperator.example.com%3E >

E.6 Query & Response Examples between the LRF & RDF

E.6.1 Query from the LRF to the RDF

```
<?xml version="1.0" encoding="UTF-8"?>
<findService xmlns="urn:ietf:params:xml:ns:lost1"
  recursive="true" serviceBoundary="value">
  <location id="627b8bf819d0bad4d" profile="civic">
    <civicAddress
      xmlns="urn:ietf:params:xml:ns:pidf:geopriv10:civicAddr">
      <country>US</country>
      <A1>Illinois</A1>
      <A3>Lisle</A3>
      <A6>Warrenville Rd</A6>
      <HNO>3030</HNO>
      <PC>60532</PC>
    </civicAddress>
  </location>
  <service>urn:service:sos.</service>
</findService>
```

E.6.2 Response to the LRF from RDF

Response for routing to a legacy emergency services network:

```
<?xml version="1.0" encoding="UTF-8"?>
<findServiceResponse xmlns="urn:ietf:params:xml:ns:lost1">
  <mapping
    expires="2011-01-01T01:44:33Z"
    lastUpdated="2010-11-01T01:00:00Z"
    source="rdf.rdfprovider.example"
    sourceId="e8b05a41d8d1415b80f2cdbb96ccf109">
    <service>urn:service:sos </service>
    <uri>sip:17735554321@carrier.example.net;user=phone/uri>
    <serviceNumber>120</serviceNumber>
  </mapping>
  <locationUsed id="627b8bf819d0bad4d"/>
  </findServiceResponse>
```

Response for routing to an ESInet:

```
<?xml version="1.0" encoding="UTF-8"?>
<findServiceResponse xmlns="urn:ietf:params:xml:ns:lost1">
  <mapping
    expires="2011-01-01T01:44:33Z"
    lastUpdated="2010-11-01T01:00:00Z"
    source="rdf.rdfprovider.example"
    sourceId="e8b05a41d8d1415b80f2cdbb96ccf109">
    <service>urn:service:sos </service>
    <uri>sip:esrp.esinet.net</uri>
    <serviceNumber>120</serviceNumber>
  </mapping>
  <locationUsed id="627b8bf819d0bad4d"/>
  </findServiceResponse>
```

E.7 SIP INVITE Sent from BGCF towards the Legacy Emergency Services Network Fixed-line UE

The following represents an example of a SIP INVITE sent from BGCF towards the legacy emergency services network for an emergency call originated from fixed-line UE:

```
INVITE sip:+17735554321@carrier.example.net;user=phone SIP/2.0
Via: SIP/2.0/UDP bgcf.carrier.example.net;branch=z9hG4bKo2c0947vk
Via: SIP/2.0/UDP e-cscf.carrier.example.net;branch=z9hG4bKvjoi09u
Via: SIP/2.0/UDP p-cscf.carrier.example.net;branch=z9hG4bK776asdhds
Via: SIP/2.0/UDP ue.carrier.example.net; branch=z9hG4bK0j4vpoJlkif50
From: <sip:+13125551234@carrier.example.net;user=phone>;tag=23ac
To: <urn:service:sos>
Contact: <sip:+13125551234@carrier.example.net;user=phone>
P-Asserted-Identity:
 <sip:+13125551234;cpc=emergency;oli=00@carrier.example.net;user=phone>
P-Charging-Vector: icid=34c23c445902;
 icid-generated-at=e-cscf.carrier.example.net;orig-ioi=carrier.example.net
Route: <sip:mgcf.carrier.example.net;lr>
Record-Route: <sip:e-cscf.carrier.example.net;lr>
Record-Route: <sip:p-cscf.carrier.example.net;lr>
Max-Forwards: 66
Call-ID: 19dn30
CSeq: 1 INVITE
Supported: 100rel
Content-Type: application/sdp
Content-Length: nn
[SDP here]
```

E.8 SIP INVITE Sent from IBCF towards the ESInet for Mobile UE

The following represents an example of a SIP INVITE sent from IBCF towards the ESInet PSAP for an emergency call originated from mobile UE. This example assumes that IBCF is acting as a SIP Proxy without THIG (Topology Hiding Interworking Gateway) functionality:

```
INVITE urn:service:sos SIP/2.0
Via: SIP/2.0/UDP IBCF.carrier.example.net;branch=z9hG4bK5690frHo0
Via: SIP/2.0/UDP e-cscf.carrier.example.net;branch=z9hG4bKvw0tlswWs
Via: SIP/2.0/UDP p-cscf.carrier.example.net;branch=z9hG4bK776asdhds
Via: SIP/2.0/UDP ue.carrier.example.net; branch=z9hG4bK5t0e45bop08
From: <sip:+13125551234@carrier.example.net;user=phone>tag=23ac
To: <urn:service:sos>
Contact: <sip:+13125551234@carrier.example.net;user=phone>
P-Asserted-Identity:<sip:+13125551234@carrier.example.net;user=phone>
Geolocation:<http:lrf.lrfprovider.net/9xkei90z> #Reference Identifier
Geolocation-Routing:yes
P-Charging-Vector: icid=34c23c445902;
 icid-generated-at=e-cscf.carrier.example.net;orig-ioi=carrier.example.net
Route: <sip:esrp.esinet.net;lr>
Record-Route: <sip:IBCF.carrier.example.net;lr>
Record-Route: <sip:e-cscf.carrier.example.net;lr>
Record-Route: <sip:p-cscf.carrier.example.net;lr>
Max-Forwards: 66
Call-ID: 19dn30
CSeq: 1 INVITE
Supported: 100rel
Content-Type: application/sdp
Content-Length: nn
[SDP here]
```

Annex F
(informative)

F Access Network Types

This annex describes some of the access network types for which the procedures and requirements in this document are applicable, with specific reference to IMS interaction, handover, and support of location. For each access type, capabilities and requirements are summarized with references to the applicable standards in which they are fully defined. Any differences to existing standards are defined here in clause 8.

F.1 LTE Access

F.1.1 Summary & References

LTE access is described and defined in 3GPP TSs 36.300 [Ref 12], 36.331 [Ref 13], 23.401 [Ref 14], and 24.301 [Ref 16]. LTE provides wireless access for both voice and low or high bandwidth data for mobile users.

F.1.2 Support of IMS Emergency Calls

LTE access supports IMS emergency voice and GTT calls as defined in 3GPP TSs 23.167 [Ref 1], 23.401 [Ref 14], and 24.229 [Ref 2].

F.1.3 Handover of IMS Emergency Calls

Handover of an IMS emergency call within one LTE access network (i.e., between different eNodeBs) is defined in 3GPP TS 23.401 [Ref 14].

Handover of an IMS emergency call from LTE to HSPA access is defined in 3GPP TS 23.401 [Ref 14].

Handover of an IMS emergency call from LTE to eHRPD access is defined in 3GPP TS 23.402 [Ref 15] and 3GPP2 X.S0057-A [Ref 17].

Single Radio Voice Call Continuity (SRVCC) of an IMS emergency voice call from LTE access to the circuit domain with either UTRAN or GERAN is defined in 3GPP TSs 23.237 [Ref 18] and 23.216 [Ref 19].

Handover applies to both normal service and limited service states.

F.1.4 Location Support for IMS Emergency Calls

Location of a UE with LTE access and an IMS emergency call may be supported using the 3GPP Control plane solution defined in 3GPP TSs 23.271 [Ref 5] and 36.305 [Ref 20]. An informative summary of this solution is provided in Annex C.1.

Location of a UE with LTE access and an IMS emergency call may also be supported using the OMA User plane solution defined in OMA-TS-ULP-V2_0 [Ref 11]. An informative summary of this solution is provided in Annex C.2.

Following handover of an IMS emergency call within an LTE access network or from LTE access to another access type, location support may be continued and the location solution may be changed as defined in 3GPP TS 23.271 [Ref 5]. An informative summary of this support is provided in Annex C.1.5.

F.2 HSPA Access

F.2.1 Summary & References

HSPA access is described and defined in 3GPP TSs 25.401 [Ref 21], 25.331 [Ref 22], 23.060 [Ref 23], and 24.008 [Ref 24]. HSPA provides wireless access for both voice and low or high bandwidth data for mobile users.

F.2.2 Support of IMS Emergency Calls

HSPA access supports IMS emergency voice and GTT calls as defined in 3GPP TSs 23.167 [Ref 1], 23.060 [Ref 23], and 24.229 [Ref 2].

F.2.3 Handover of IMS Emergency Calls

Handover of an IMS emergency call within one HSPA access network (i.e., between different Node Bs) is defined in 3GPP TS 23.060 [Ref 23].

Handover of an IMS emergency call from HSPA to LTE access is defined in 3GPP TS 23.401 [Ref 14].

Single Radio Voice Call Continuity (SRVCC) of an IMS emergency voice call from HSPA access to the circuit domain with either UTRAN or GERAN is defined in 3GPP TSs 23.237 [Ref 18] and 23.216 [Ref 19].

Handover support applies to both normal service and limited service states.

F.2.4 Location Support for IMS Emergency Calls

Location of a UE with HSPA access and an IMS emergency call may be supported using the 3GPP Control plane solution defined in 3GPP TSs 23.271 [Ref 5] and 25.305 [Ref 25]. An informative summary of this solution is provided here in Annex C.1.

Location of a UE with HSPA access and an IMS emergency call may also be supported using the OMA User plane solution defined in OMA-TS-ULP-V2_0 [Ref 11]. An informative summary of this solution is provided here in Annex C.2.

Following handover of an IMS emergency call within an HSPA access network or from HSPA access to another access type, location support may be continued and the location solution may be changed as defined in 3GPP TS 23.271 [Ref 5]. An informative summary of this support is provided in Annex C.1.5.

Annex G
(informative)

G Use Case

This annex describes a set of use cases for an IMS emergency call origination that include use of fixed and mobile UEs, legacy as well as IP capable PSAPs, routing on geographic location or cell site/sector, and use of location-by-value or location-by-reference. The following use cases apply to media types of voice, text, and video when a "call" is defined generically: G2, G4, G6, G8, and G10. Use cases G1, G3, G5, G7, G9, and G11 apply for voice and text to legacy emergency services network.

G.1 IMS Emergency Call with Location Value Routed to a Legacy PSAP via a Legacy Emergency Services Network

Short Description

The origination network receives an emergency call/session request containing a location value from an originating device/User Equipment (UE). The call is routed via a legacy Emergency Services Network to a legacy PSAP and the PSAP has to query for location information.

Actors

Bob is the caller whose UE originated the emergency call.

Carol is the PSAP call taker at a legacy PSAP to which the emergency call is delivered.

Pre-Conditions

Bob's UE has obtained its location using a mechanism that is beyond the scope of this document. The location is assumed to be "routable".

Post-Conditions

Carol is in communication with Bob and is viewing his location information.

Normal Flow

1. Bob initiates an emergency call and the call request is forwarded to the originating network along with Bob's location information.
2. The origination network uses the location information provided with the emergency call request to determine the routing for the call.
3. The originating network caches Bob's location information and creates a Reference Identifier.
4. The originating network routes the call toward the legacy emergency services network, passing the Reference Identifier for delivery to Carol's PSAP.
5. Carol answers the call.
6. In parallel, Carol's call handling equipment uses the Reference Identifier to query for Bob's location information.
7. Bob's location information and callback information are returned and displayed on Carol's Customer Premises Equipment (CPE).

G.2 IMS Emergency Call with Location Value Routed to an ESInet

Short Description

The origination network receives an emergency call/session request containing a location value from an originating device/UE. The call is routed to a NENA i3 PSAP via a NENA i3 ESInet, and the location and callback information are delivered with the call.

Actors

Bob is the caller whose UE originated the emergency call.

Carol is the PSAP call taker at a NENA i3 PSAP to which the emergency call is delivered.

Pre-Conditions

Bob's UE has obtained its location using a mechanism that is beyond the scope of this document. The location is assumed to be "routable".

Post-Conditions

Carol is in communication with Bob and is viewing Bob's location information.

Normal Flow

1. Bob initiates an emergency call and the call request is forwarded to the originating network along with Bob's location information.
2. The origination network uses the location information provided in the emergency call request to determine the routing for the call.
3. The originating network routes the call toward the ESInet (passing the location-by-value and callback information received in the emergency call request) for delivery to Carol's PSAP.
4. Carol answers the call and Bob's location information is displayed on her CPE.

G.3 IMS Emergency Call with a "Telephone Number" Routed to a Legacy PSAP via a Legacy Emergency Services Network

Short Description

A call is initiated from a fixed UE that includes a "telephone number" in its emergency call/session request (and no location reference or location value). The originating network uses the telephone number to obtain location associated with the caller's registered address and then caches it. The originating network creates a Reference Identifier and associates it with the location information. The origination network routes the call toward a legacy PSAP via a legacy Emergency Services Network, with the Reference Identifier. The PSAP uses the Reference Identifier to query for location information.

Actors

Bob is the caller whose fixed UE originated the emergency call.

Carol is the PSAP call taker at a legacy PSAP to which the emergency call is delivered.

Pre-Conditions

An association between Bob's telephone number and the location associated with Bob's registered address has been pre-provisioned in the originating network.

Post-Conditions

Carol is in communication with Bob and is viewing his location and callback information.

Normal Flow[14]

1. Bob initiates an emergency call and the call request containing Bob's telephone number (and no location reference or location value) is forwarded to the originating network.
2. The originating network uses the telephone number to obtain the location associated with Bob's registered address.
3. The originating network uses the location to determine the routing for the call.
4. The originating network caches Bob's location information and creates a Reference Identifier.
5. The originating network routes the call toward the legacy emergency services network, passing the Reference Identifier for delivery to Carol's PSAP.
6. Carol answers the call.
7. In parallel, Carol's call handling equipment uses the Reference Identifier to query for Bob's location information.
8. Bob's location information and callback information are returned and displayed on Carol's CPE.

Alternate Flow[15]

1. Bob initiates an emergency call and the call request containing Bob's telephone number is forwarded to the originating network.
2. The originating network uses the telephone number to obtain the location associated with Bob's registered address.
3. The originating network uses the location to determine the routing for the call.
4. The originating network routes the call toward the legacy emergency services network, passing the telephone number received in the emergency call request for delivery to Carol's PSAP.
5. Carol answers the call.
6. In parallel, Carol's call handling equipment uses the telephone number to query an ALI system for Bob's location information.
7. Bob's location information and callback information are displayed on Carol's CPE.

G.4 IMS Emergency Call with a "Telephone Number" Routed to an ESInet

Short Description

A call is initiated from a fixed UE that includes a "telephone number" in its emergency call/session request (and no location reference or location value). The call is routed toward a NENA i3 PSAP via an ESInet, and the location and callback information are delivered with the call.

Actors

Bob is the caller whose fixed UE originated the emergency call.

Carol is the PSAP call taker at a NENA i3 PSAP to which the emergency call is delivered.

Pre-Conditions

An association between Bob's telephone number and the location associated with Bob's registered address has been pre-provisioned in the originating network.

[14] This flow assumes that a Reference Identifier is created that is different from the telephone number.

[15] This flow assumes that the telephone number is the Reference Identifier and no additional query key is created.

Post-Conditions

Carol is in communication with Bob and is viewing Bob's location and callback information.

Normal Flow

1. Bob initiates an emergency call and the call request containing Bob's telephone number (and no location reference or location value) is forwarded to the originating network.
2. The originating network uses the telephone number to obtain the location associated with Bob's registered address.
3. The originating network uses the location to determine the routing for the call.
4. The originating network routes the call toward the NENA i3 ESInet (passing the location-by-value and the telephone number received in the emergency call request) for delivery to Carol's PSAP.
5. Carol answers the call and Bob's location and callback information are displayed on her CPE.

G.5 IMS Emergency Call with MDN/MSISDN & Cell Site/Sector Information Routed to a Legacy PSAP via a Legacy Emergency Services Network

Short Description

The origination network receives an emergency call/session request containing the MDN/MSISDN and cell site/sector information from an originating device/UE. The originating network uses available information (e.g., pre-provisioned originating cell site/sector identifier) to determine the routing for the call. The origination network creates a Reference Identifier for the call, and associates it with the MDN/MSISDN and cell site/sector ID. In parallel, the originating network attempts to acquire a more accurate location. The PSAP has to query for this information. The call is delivered to a legacy PSAP along with the Reference Identifier. The PSAP has to query for location information and may also query for location updates.

Actors

Bob is the caller whose mobile UE originated the emergency call.

Carol is the PSAP call taker at a legacy PSAP to which the emergency call is delivered.

Pre-Conditions

The operator has a mechanism to determine the routing based on the cell site/sector (e.g., bilateral agreement between the service provider [or its 3rd party partner] and the PSAP, which takes into account that the location of the cell site/sector or access point may not be in the physical boundaries of the PSAP).

Post-Conditions

Carol is in communication with Bob and viewing his location and callback information.

Normal Flow

1. Bob initiates an emergency call request with the serving originating network and the call request includes the MDN/MSISDN and cell site/sector information.
2. The originating network uses the information provided in the emergency call request to determine the appropriate PSAP/routing for the call.
3. The originating network creates a Reference Identifier and associates it with the MDN/MSISDN and cell site/sector information received in the emergency call request.
4. The originating network initiates the location acquisition process.
5. The originating network routes the call toward the legacy emergency services network, passing the Reference Identifier for delivery to Carol's PSAP.

6. Carol answers the call.
7. In parallel, Carol's call handling equipment uses the Reference Identifier and queries an ALI system for Bob's location information.
8. The originating network returns Bob's available location information (e.g., most likely cell site/sector) and callback information, and they are displayed on Carol's CPE.
9. The originating network completes its location acquisition process.
10. Carol may subsequently retrieve the updated location using the same Reference Identifier.
11. Bob's location information is updated (if available) and the updated/last known location is displayed on Carol's CPE.

Alternate Flow[16]

1. Bob initiates an emergency call request with the serving originating network and the call request includes the MDN/MSISDN and cell site/sector information.
2. The originating network uses the information provided in the emergency call request to determine the appropriate PSAP/routing for the call.
3. The originating network creates a Reference Identifier and associates it with the MDN/MSISDN and cell site/sector information received in the emergency call request.
4. The originating network initiates the location acquisition process.
5. The originating network routes the call toward the legacy emergency services network, passing the Reference Identifier for delivery to Carol's PSAP.
6. Carol answers the call.
7. In parallel, Carol's call handling equipment uses the Reference Identifier and queries an ALI system for Bob's location information.
8. The ALI system steers the location query to the origination network.
9. Having completed the location acquisition process, the originating network returns Bob's last known location information and callback information, and they are displayed on Carol's CPE.
10. Carol may subsequently request updated location using the same Reference Identifier.
11. The originating network returns the updated/last known location and it is displayed in Carol's CPE.

G.6 IMS Emergency Call with MDN/MSISDN & Cell Site/Sector Information Routed to an ESInet

Short Description

The origination network receives an emergency call/session request containing the MDN/MSISDN and cell site/sector information from an originating device/UE. The originating network uses available information (e.g., pre-provisioned originating cell site/sector identifier) to determine routing for the call. The originating network creates a Reference Identifier for the call, and associates it with the MDN/MSISDN and cell site/sector ID. In parallel, the originating network attempts to acquire a more accurate location. The call is delivered to an ESInet along with the Reference Identifier. The PSAP has to query for location information and may also query for location updates.

Actors

Bob is the caller whose mobile UE originated the emergency call.

Carol is the PSAP call taker at a NENA i3 PSAP to which the emergency call is delivered.

[16] This flow applies when Bob's location comes back on the initial query.

Pre-Conditions

The operator has a mechanism to determine the routing based on the cell site/sector (e.g., bilateral agreement between the service provider [or its 3rd party partner] and the PSAP, which takes into account that the location of the cell site/sector or access point may not be in the physical boundaries of the PSAP).

Post-Conditions

Carol is in communication with Bob and viewing his location and callback information.

Normal Flow

1. Bob initiates an emergency call request with the serving originating network and the call request includes the MDN/MSISDN and cell site/sector information.
2. The originating network uses the information provided in the emergency call request to determine the appropriate PSAP/routing for the call.
3. The originating network creates a Reference Identifier and associates it with the MDN/MSISDN and the cell site/sector information received in the emergency call request.
4. The originating network initiates the location acquisition process.
5. The originating network routes the call toward the NENA i3 ESInet, passing the Reference Identifier and the MDN/MSISDN received in the emergency call request for delivery to Carol's PSAP.
6. Carol answers the call.
7. In parallel, Carol's call handling equipment dereferences with the origination network (including the Reference Identifier created by the originating network in the dereference request) to acquire Bob's location information.
8. The originating network returns Bob's available location information (e.g., most likely cell site/sector expressed as a location value) and it is displayed (along with the MDN/MSISDN received in the emergency call request) on Carol's CPE.
9. The originating network completes its location acquisition process.
10. Carol may subsequently retrieve the updated location by dereferencing with the originating network using the same Reference Identifier.
11. Bob's location information is updated (if available) and the updated/last known is displayed on Carol's CPE.

Alternate Flow[17]

1. Bob initiates an emergency call request with the serving originating network and the call request includes the MDN/MSISDN and cell site/sector information.
2. The originating network uses the information provided in the emergency call request to determine the appropriate PSAP/routing for the call.
3. The originating network creates a Reference Identifier and associates it with the MDN/MSISDN and the cell site/sector information received in the emergency call request.
4. The originating network initiates the location acquisition process.
5. The originating network routes the call toward the NENA i3 ESInet, passing the Reference Identifier and the MDN/MSISDN received in the emergency call request for delivery to Carol's PSAP.
6. Carol answers the call.
7. In parallel, Carol's call handling equipment dereferences with the origination network (including the Reference Identifier created by the originating network in the dereference request) to acquire Bob's location information.
8. Having completed the location acquisition process, the originating network returns Bob's last known location information (expressed as a location value), and it is displayed (along with the MDN/MSISDN received in the emergency call request) on Carol's CPE.

[17] This flow applies when Bob's location comes back on the initial query.

9. Carol may subsequently retrieve updated location by de-referencing with the originating network using the same Reference Identifier.
10. The originating network returns the updated/last known location and it is displayed in Carol's CPE.

G.7 IMS Emergency Call with Location Reference URI Routed to a Legacy PSAP via a Legacy Emergency Services Network Short Description

NOTE: UE provided location-by-reference is not specified in this version of the standard.

Short Description

The origination network receives an emergency call/session request containing location reference URI from an originating device/User Equipment (UE). The originating network queries a location server in the Access Network for the UE location to support call routing. The origination network creates a Reference Identifier for the call, and associates it with the location reference URI and the received de-referenced location value. The origination network routes the call via a legacy emergency services network to a legacy PSAP. The call is delivered to the legacy PSAP with the Reference Identifier created by the origination network. The PSAP has to query for location information and may also query for location updates.

Actors

Bob is the caller whose mobile UE originated the emergency call.

Carol is the PSAP call taker at a legacy PSAP to which the emergency call is delivered.

Pre-Conditions

Bob's UE has access to a location server in the Access Network that is able to deliver a location reference URI and supports a mechanism to obtain that location reference URI.

The operator of the origination network has access to the location server in the Access Network that generated the location reference URI and supports a mechanism by which it can de-reference a received location reference URI to obtain a location value.

Post-Conditions

Carol is in communication with Bob and viewing his location and callback information.

Normal Flow

1. Bob's UE interacts with a location server in an Access Network to obtain a location reference URI (R1).
2. Bob initiates an emergency call request with the serving originating network and the call request includes a location reference URI (R1), including the location reference R1 in the de-reference request.
3. The origination network queries the location server that generated location reference URI R1 for the location of Bob's UE using the location reference R1.
4. The origination network uses the location value provided by the location server in response to the de-reference request determine the routing for the call.
5. The origination network caches Bob's location and location reference URI R1 and creates a Reference Identifier R2.
6. The origination network routes the call toward the legacy emergency services network passing Reference Identifier R2 for delivery to Carol's PSAP.
7. Carol answers the call.
8. In parallel, Carol's call handling equipment uses Reference Identifier R2 to query the origination network for Bob's initial location.

9. Bob's location cached in Step 5 and callback information are returned and displayed on Carol's Customer Premises Equipment (CPE).
10. At some later time, Carol's call handling equipment uses Reference Identifier R2 to query the origination network for updated location for Bob's UE.
11. The origination network de-references with the location server that created the original location reference URI for the location of Bob's UE using the location reference URI R1.
12. The location of Bob's UE is obtained by the location server and returned to Carol via the origination network and Carol's call handling equipment.

G.8 IMS Emergency Call with Location Reference URI Routed to an ESInet Short Description

NOTE: UE provided location-by-reference is not specified in this version of the standard.

Short Description

The origination network receives an emergency call/session request containing location reference URI from an originating device/User Equipment (UE). The originating network queries a location server in the Access Network for the UE location to support call routing. The origination network delivers the call to the NENA i3 ESInet with the location reference URI received from the UE. The NENA i3 ESInet de-references the location URI with the location server that generated it to obtain a location value to support call routing. The ESInet delivers the call to the PSAP with the location reference URI provided by the UE. The PSAP must de-reference the location reference URI with the location server that created it to obtain location information for the call. The PSAP may also initiate a subsequent de-reference request to obtain location updates.

Actors

Bob is the caller whose mobile UE originated the emergency call.

Carol is the PSAP call taker at a NENA i3 PSAP to which the emergency call is delivered.

Pre-Conditions

Bob's UE has access to a location server in the Access Network that is able to deliver a location reference URI and supports a mechanism to obtain that location reference URI.

The operator of the origination network has access to the location server in the Access Network that generated the location reference URI and supports a mechanism by which it can de-reference a received location reference URI to obtain a location value.

The operator of the ESInet (on behalf of the PSAP Authority) has access to the location server in the Access Network that generated the location reference URI and supports a mechanism by which it can de-reference a received location reference URI to obtain a location value.

Post-Conditions

Carol is in communication with Bob and viewing his location and callback information.

Normal Flow

1. Bob's UE interacts with a location server in an Access Network to obtain a location reference URI (R1).
2. Bob initiates an emergency call request with the serving originating network and the call request includes a location reference URI (R1).
3. The origination network queries the location server that generated location reference URI R1 for the location of Bob's UE, including the location reference R1 in the de-reference request.

4. The origination network uses the location value provided by the location server in response to the de-reference request determine the routing for the call.
5. The origination network routes the call toward the NENA i3 ESInet passing location reference URI R1.
6. The NENA i3 ESInet de-references with the location server that created the location reference URI to obtain routing location, including location reference URI R1 in the de-reference request.
7. The NENA i3 ESInet uses the received location value to route the call, and delivers the call to the PSAP with location reference URI R1 and the callback number.
8. Carol answers the call.
9. In parallel, Carol's call handling equipment initiates a de-reference request with the location server in the Access Network, using location reference URI R1, to obtain Bob's location.
10. Bob's location is returned and displayed on Carol's Customer Premises Equipment (CPE).
11. At some later time, Carol's call handling equipment uses location reference URI R1 to de-reference with the location server in the Access Network for updated location for Bob's UE.
12. The location of Bob's UE is obtained by the location server and returned to Carol via Carol's call handling equipment.

G.9 IMS Emergency Call with Network Acquired Mobile Location Routed to a Legacy PSAP via a Legacy Emergency Services Network

Short Description

The origination network receives an emergency call/session request that contains MSISDN and IMEI but not the location information. The originating network acquires a mobile location of the UE. A Reference Identifier is created and the call is routed via a legacy emergency services network to a legacy PSAP and the PSAP has to query for location information.

Actors

Bob is the caller whose UE originated the emergency call.

Carol is the PSAP call taker at a legacy PSAP to which the emergency call is delivered.

Pre-Conditions

None

Post-Conditions

Carol is in communication with Bob and is viewing his location information.

Normal Flow

1. Bob initiates an emergency call and the call request is forwarded to the originating network.
2. The origination network acquires Bob's mobile location and uses it to determine the routing for the call.
3. The originating network caches Bob's location information and creates a Reference Identifier.
4. The originating network routes the call toward the legacy emergency services network, passing the Reference Identifier for delivery to Carol's PSAP.
5. Carol answers the call.
6. In parallel, Carol's call handling equipment uses the Reference Identifier to query for Bob's location information.
7. Bob's location information and callback information are returned and displayed on Carol's Customer Premises Equipment (CPE).

8. Subsequently, Carol may request an updated location using the Reference Identifier and the network will reacquire Bob's current location and return it to Carol.

G.10 IMS Emergency Call with Network Acquired Mobile Location Routed to an ESInet by Reference

Short Description

The origination network receives an emergency call/session request that contains MSISDN and IMEI but not the location information. The originating network acquires a mobile location of the UE. A Reference Identifier is created and the call is routed to a NENA i3 PSAP via a NENA i3 ESInet, and PSAP queries for location.

Actors

Bob is the caller whose UE originated the emergency call.

Carol is the PSAP call taker at a NENA i3 PSAP to which the emergency call is delivered.

Pre-Conditions

None

Post-Conditions

Carol is in communication with Bob and is viewing Bob's location information.

Normal Flow

1. Bob initiates an emergency call and the call request is forwarded to the originating network.
2. The origination network acquires Bob's mobile location and uses the location information to determine the routing for the call.
3. The originating network caches Bob's location information and creates a location reference URI.
4. The originating network routes the call toward the ESInet (passing the location reference URI in the emergency call request) for delivery to Carol's PSAP.
5. Carol answers the call.
6. In parallel, Carol's call handling equipment uses the location reference URI to query for Bob's location information.
7. Bob's location information is returned and displayed on Carol's call handling equipment.
8. Subsequently, Carol may request an updated location using the location reference URI and the network will reacquire Bob's current location and return it to Carol.

G.11 IMS Call Received from a Mobile UE with Location Information but without a Valid Callback Number, & Routed to a Legacy PSAP via a Legacy Emergency Services Network

Short Description

The origination network receives an emergency call/session request containing location information (i.e., a location reference URI or cell site/sector-based location information) and no callback information from an originating mobile device/UE that does not have a valid callback number associated with it. For North America, the E-CSCF includes a non-dialable callback number (following the mechanism specified in 3GPP TS 24.229 [Ref 2]) in the emergency session request forwarded to the LRF. The originating network uses the location information provided in the emergency session request to acquire or derive a routing location that will be used to determine the routing for the call. The origination network creates a Reference Identifier for the call, and associates it with the non-dialable

callback number and location information provided in the emergency session request. In parallel the originating network attempts to acquire a more accurate dispatch location. The PSAP has to query for this information. The call is delivered to a legacy PSAP along with the Reference Identifier and/or the non-dialable callback number, as appropriate. The PSAP has to query for location information and may also query for location updates.

Actors

Bob is the caller whose mobile UE originated the emergency call.

Carol is the PSAP call taker at a legacy PSAP to which the emergency call is delivered.

Pre-Conditions

The operator has a mechanism to determine the non-dialable callback number, as well as the routing based on a routing location acquired/derived from the location information provided in the emergency session request.

Post-Conditions

Carol is in communication with Bob and viewing his location and callback information.

Normal Flow

1. Bob initiates an emergency call request from a device which has no valid callback number associated with it. The call request is delivered to the serving originating network with location information but no callback information.
2. For North America, the originating network generates a non-dialable callback number per Annex C of J-STD-036-C-2 [Ref 7].
3. The originating network uses the information provided in the emergency call request to acquire/derive a routing location for the call, then it uses this routing location to determine the appropriate PSAP/routing for the call.
4. The originating network creates a Reference Identifier (R1) and associates it with the non-dialable callback number and the location information received in the emergency call request.
5. If the received emergency session request contains cell site/sector-based location information, the originating network initiates the location acquisition process. If the received emergency session request contains a location reference URI, this step is omitted.
6. The originating network routes the call toward the legacy emergency services network passing the Reference Identifier (R1) and, if appropriate, the non-dialable callback number, for delivery to Carol.
7. Carol answers the call.
8. In parallel, Carol's call handling equipment uses the Reference Identifier (R1) to query an ALI system for Bob's location information.
9. The originating network returns Bob's available location information and the non-dialable callback number, and they are displayed on Carol's CPE.
10. If initiated in Step 5, the originating network completes its location acquisition process.
11. Carol may subsequently retrieve updated location using the same Reference Identifier (R1).
12. Bob's location information is updated (if available from Step 10 or via subsequent de-referencing of the location reference URI) and the updated/last known location is displayed on Carol's CPE.

Alternate Flow[18]

1. Bob initiates an emergency call request from a device which has no valid callback number associated with it. The call request is delivered to the serving originating network with location information but no callback information.
2. For North America, the originating network generates a non-dialable callback number per Annex C of J-STD-036-C-2 [Ref 7].
3. The originating network uses the information provided in the emergency call request to acquire/derive a routing location for the call, then it uses this routing location to determine the appropriate PSAP/routing for the call.
4. The originating network creates a Reference Identifier (R1) and associates it with the non-dialable callback number and the location information received in the emergency call request.
5. If the received emergency session request contains cell site/sector-based location information, the originating network initiates the location acquisition process. If the received emergency session request contains a location reference URI, this step is omitted.
6. The originating network routes the call toward the legacy emergency services network passing the Reference Identifier (R1) and, if appropriate, the non-dialable callback number, for delivery to Carol.
7. Carol answers the call.
8. In parallel, Carol's call handling equipment uses the Reference Identifier (R1) and queries an ALI system for Bob's location information.
9. The ALI system steers the location query to the origination network.
10. Having completed the location acquisition/de-reference process, the originating network returns Bob's last known location information and the non-dialable callback number, and they are displayed on Carol's CPE.
11. Carol may subsequently request updated location using the same Reference Identifier.
12. The originating network returns the updated/last known location and it is displayed in Carol's CPE.

G.12 IMS Call Received from a Mobile UE with Location Information but without a Valid Callback Number & Routed to an ESInet

Short Description

The origination network receives an emergency call/session request containing location information (i.e., a location reference URI, cell site/sector-based location information) and no callback information from an originating mobile device/UE that does not have a valid callback number associated with it. For North America, the E-CSCF includes a non-dialable callback number (following the mechanism specified in 3GPP TS 24.229 [Ref 2]) in the emergency session request forwarded to the LRF. The originating network uses the location information provided in the emergency session request to acquire or derive a routing location that will be used to determine the routing for the call. If the incoming emergency session request contains cell site/sector-based location information, the origination network creates a Reference Identifier for the call, associates it with the non-dialable callback number and location information provided in the emergency session request, and passes it as a location reference URI to the NENA i3 ESInet. If the incoming emergency session request contains a location reference URI, the originating network passes the location reference URI received in the emergency session request and the non-dialable callback number to the NENA i3 ESInet. If the originating network creates a Reference Identifier, it will also attempt to acquire a more accurate dispatch location, in parallel. The NENA i3 ESInet has to query for routing location using the Reference Identifier or location reference URI. The call is delivered to the NENA i3 PSAP along with the location reference URI and the non-dialable callback number. The NENA i3 PSAP has to query for dispatch location using the location reference URI and may also query for location updates.

[18] This flow applies when Bob's location comes back on the initial query.

Actors

Bob is the caller whose mobile UE originated the emergency call.

Carol is the PSAP call taker at a NENA i3 PSAP to which the emergency call is delivered.

Pre-Conditions

The operator has a mechanism to determine the non-dialable callback number, as well as the routing based on a routing location acquired/derived from the location information provided in the emergency session request.

Post-Conditions

Carol is in communication with Bob and viewing his location and callback information.

Normal Flow

1. Bob initiates an emergency call request from a device which has no valid callback number associated with it. The call request is delivered to the serving originating network with location information but no callback information.
2. For North America, the originating network generates a non-dialable callback number per Annex C of J-STD-036-C-2 [Ref 7].
3. The originating network uses the information provided in the emergency call request to acquire/derive a routing location for the call, then it uses this routing location to determine the appropriate PSAP/routing for the call.
4. If the received emergency session request contains cell site/sector-based location information, the originating network creates a Reference Identifier (R1) and associates it with the non-dialable callback number and the cell site/sector information received in the emergency call request. If the received emergency session request contains a location reference URI (R2), this step is omitted.
5. If the received emergency session request contains cell site/sector-based location information, the originating network initiates the location acquisition process. If the received emergency session request contains a location reference URI, this step is omitted.
6. The originating network routes the call toward the NENA i3 ESInet, passing a location reference URI and the non-dialable callback number for delivery to Carol. If the received emergency session request contains cell site/sector-based location information, the location reference URI will contain the Reference Identifier (R1) created by the originating network. If the received emergency session request contains a location reference URI, the location reference URI delivered to the NENA i3 ESInet/PSAP will be as received in the initial emergency session request (R2).
7. Carol answers the call.
8. In parallel, Carol's call handling equipment initiates a de-reference request with the element identified in the location reference URI to acquire Bob's dispatch location. (If the location reference URI contains R1, it will de-reference with the origination network. If the location reference URI contains R2, it will de-reference with a location server in the Access Network.)
9. Bob's available location information is returned in response to the de-reference request and is displayed (along with the non-dialable callback number received in the emergency call request) on Carol's CPE.
10. If initiated in Step 5, the originating network completes its location acquisition process.
11. Carol may subsequently retrieve the updated location by initiating a de-reference request using the same location reference URI as received in Step 6.
12. Bob's location information is updated (if available) and the updated/last known is displayed on Carol's CPE.

Alternate Flow[19]

1. Bob initiates an emergency call request from a device which has no valid callback number associated with it. The call request is delivered to the serving originating network with location information but no callback information.
2. For North America, the originating network generates a non-dialable callback number per Annex C of J-STD-036-C-2 [Ref 7].
3. The originating network uses the information provided in the emergency call request to acquire/derive a routing location for the call, then it uses this routing location to determine the appropriate PSAP/routing for the call.
4. If the received emergency session request contains cell site/sector-based location information, the originating network creates a Reference Identifier (R1) and associates it with the non-dialable callback number and the cell site/sector information received in the emergency call request. If the received emergency session request contains a location reference URI (R2), this step is omitted.
5. If the received emergency session request contains cell site/sector-based location information, the originating network initiates the location acquisition process. If the received emergency session request contains a location reference URI, this step is omitted.
6. The originating network routes the call toward the NENA i3 ESInet, passing a location reference URI and the non-dialable callback number for delivery to Carol. If the received emergency session request contains cell site/sector-based location information, the location reference URI will contain the Reference Identifier (R1) created by the originating network. If the received emergency session request contains a location reference URI, the location reference URI delivered to the NENA i3 ESInet/PSAP will be as received in the initial emergency session request (R2).
7. Carol answers the call.
8. In parallel, Carol's call handling equipment initiates a de-reference request with the element identified in the location reference URI to acquire Bob's dispatch location. (If the location reference URI contains R1, it will de-reference with the origination network. If the location reference URI contains R2, it will de-reference with a location server in the Access Network.)
9. The element that receives the de-reference request returns Bob's last known location information (expressed as a location value), and it is displayed (along with the non-dialable callback number received in the emergency call request) on Carol's CPE.
10. Carol may retrieve updated location information by initiating a subsequent de-reference request using the same location reference URI as received in Step 6.
11. Updated/last known location is returned in the de-reference response and is displayed in Carol's CPE.

G.13 Adding Multimedia to an Existing Emergency Call

Short Description

The caller is in voice discussion with the call taker about an incident and states that he/she has a picture (or video clip) relating to the incident that can be sent to the PSAP. The call taker tells the caller to send the picture (or video clip). The dialog regarding the incident continues as the call taker views the picture (or video clip).

Actors

Bob is the caller who originated the call.

Carol is the PSAP call taker at a NENA i3 PSAP who is in discussion with Bob regarding the incident.

[19] This flow applies when Bob's location comes back on the initial query.

Pre-Conditions

Bob and Carol are in voice discussion regarding the incident.

Post-Conditions

Carol is in communication with Bob and is viewing Bob's location, callback information and picture (or video clip).

Normal Flow

1. Bob and Carol are in voice communication regarding the incident and Bob states that he has a picture (or video clip) of the incident.
2. Carol tells Bob to send the picture (or video clip).
3. Bob selects and sends the picture (or video clip).
4. Carol receives the picture (or video clip) and continues dialog with Bob regarding the incident while viewing the picture (or video clip).

Annex H
(informative)

H Location-by-Reference

NOTE: UE provided location-by-reference is not specified in this version of the standard.

Figure H.1 illustrates NENA i3 ESInet termination where location-by-reference is provided by the UE and delivered to the NENA i3 ESInet, showing key elements within a NENA i3 ESInet that are relevant to the call flow. This call flow assumes that the ESInet and PSAP are allowed to access the location server in the Access Network that generated the location reference URI and supports a mechanism by which it can de-reference a received location reference URI to obtain a location value[20].

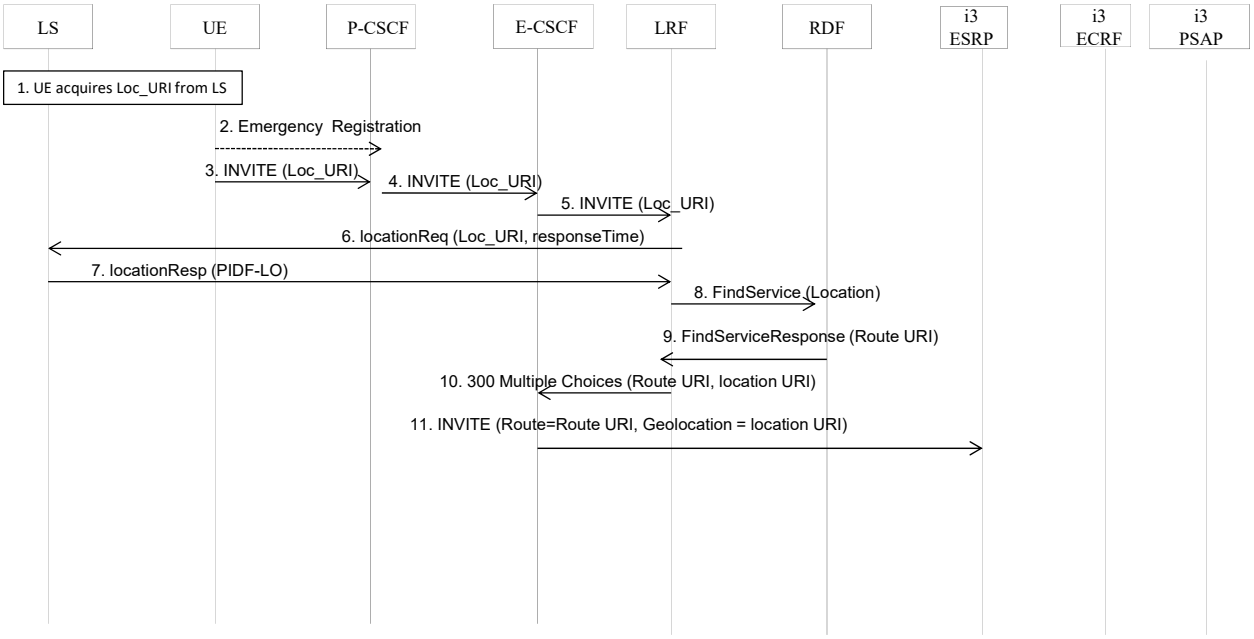

Figure H.1 – UE Location-Routed Call Delivery to NENA i3 ESInet – Location-by-Reference provided by UE

Step 1. The UE interacts with a location server in an Access Network to obtain a location reference URI.

Step 2. (Conditional) Emergency registration occurs (if not already emergency registered and has credentials).

Step 3. The UE sends a SIP INVITE containing a location reference URI to the P-CSCF.

Step 4. The P-CSCF, detecting an emergency call, forwards the SIP INVITE to the E-CSCF.

Step 5. The E-CSCF queries the LRF for location and/or route, by forwarding the SIP INVITE.

Step 6. The LRF interacts with the LS that generated the location reference URI to acquire location, including the location reference URI in the de-reference request.

Step 7. The LS responds with location value in a PIDF-LO.

Step 8. The LRF queries the RDF for routing information using the location value provided in Step 7.

Step 9. The RDF responds by providing a Route URI.

Step 10. The LRF replies to the E-CSCF with location information (the location reference URI received in the incoming SIP INVITE, in this example) and a Route URI that will direct the call toward the ESInet.

[20] These assumptions are consistent with the definition of the NENA i3 Solution provided in NENA-STA-010 [Ref 100].

Step 11. The E-CSCF forwards the SIP INVITE (with any location information received from the LRF; in this example a location reference URI) to the ESRP via an IBCF.