ETSI ES 203 283 V1.1.1 (2017-11)

Protocol specifications for Emergency Service Caller Location determination and transport

Reference
DES/NTECH-00025-M493-protocols

Keywords
emergency, location, VoIP

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This ETSI Standard (ES) has been produced by ETSI Technical Committee Network Technologies (NTECH).

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

The present document describes the protocol specifications for emergency service caller location determination and transport architecture as specified in ETSI ES 203 178 [1].

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are necessary for the application of the present document.

[1] ETSI ES 203 178: "Functional architecture to support European requirements on emergency caller location determination and transport".

[2] OMA-TS-MLP-V3_5: "Mobile Location Protocol Version 3.5".

NOTE: Available at http://www.openmobilealliance.org/release/MLS/V1_4-20150224-C/OMA-TS-MLP-V3_5-20150224-C.pdf.

[3] IETF RFC 3261: "SIP: Session Initiation Protocol".

[4] IETF RFC 4320: "Actions Addressing Identified Issues with the Session Initiation Protocol's (SIP) Non-INVITE Transaction".

[5] IETF RFC 5393: "Addressing an Amplification Vulnerability in Session Initiation Protocol (SIP) Forking Proxies".

[6] IETF RFC 5954: "Essential Correction for IPv6 ABNF and URI Comparison in RFC 3261".

[7] IETF RFC 6442: "Location Conveyance for the Session Initiation Protocol".

[8] IETF RFC 4566: "SDP: Session Description Protocol".

[9] IETF RFC 3264: "An Offer/Answer Model with the Session Description Protocol (SDP)".

[10] ETSI TS 124 229: "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3 (3GPP TS 24.229)".

[11] ETSI TS 129 165: "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; Inter-IMS Network to Network Interface (NNI) (3GPP TS 29.165)".

[12] ETSI TS 123 167: "Universal Mobile Telecommunications System (UMTS); LTE; IP Multimedia Subsystem (IMS) emergency sessions (3GPP TS 23.167)".

[13] ETSI ES 283 035: "Network Technologies (NTECH); Network Attachment; e2 interface based on the DIAMETER protocol".

[14] ETSI TS 129 163: "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; Interworking between the IP Multimedia (IM) Core Network (CN) subsystem and Circuit Switched (CS) networks (3GPP TS 29.163)".

[15] IETF RFC 4119: "A Presence-based GEOPRIV Location Object Format".

[16] IETF RFC 5139: "Revised Civic Location Format for Presence Information Data Format Location Object (PIDF-LO)".

[17] IETF RFC 5491: "GEOPRIV Presence Information Data Format Location Object (PIDF-LO) Usage Clarification, Considerations, and Recommendations".

[18] IETF RFC 6848: "Specifying Civic Address Extensions in the Presence Information Data Format Location Object (PIDF-LO)".

[19] IETF RFC 7216: "Location Information Server (LIS) Discovery Using IP Addresses and Reverse DNS".

[20] IETF RFC 5985: "HTTP-Enabled Location Delivery (HELD)".

[21] IETF RFC 5986: "Discovering the Local Location Information Server (LIS)".

[22] IETF RFC 6155: "Use of Device Identity in HTTP-Enabled Location Delivery (HELD)".

[23] IETF RFC 6915: "Flow Identity Extension for HTTP-Enabled Location Delivery (HELD)".

[24] IETF RFC 7840: "A Routing Request Extension for the HTTP-Enabled Location Delivery (HELD) Protocol".

[25] IETF RFC 6753: "A Location Dereference Protocol Using HTTP-Enabled Location Delivery (HELD)".

[26] IETF RFC 5031: "A Uniform Resource Name (URN) for Emergency and Other Well-Known Services".

[27] IETF RFC 6881: "Best Current Practice for Communications Services in Support of Emergency Calling".

[28] IETF RFC 3325: "Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks".

[29] IETF RFC 7852: "Additional Data Related to an Emergency Call".

[30] IETF RFC 3323: "A Privacy Mechanism for the Session Initiation Protocol (SIP)".

[31] IETF RFC 5079: "Rejecting Anonymous Requests in the Session Initiation Protocol (SIP)".

[32] Recommendation ITU-T Q.850 (1998) Amd. 1 (07/2001): "Usage of cause and location in the Digital Subscriber Signalling System No. 1 (DSS1) and the Signalling System No. 7 ISDN user part (ISUP), Amendment 1".

[33] ETSI TS 124 525: "Universal Mobile Telecommunications System (UMTS); LTE; Business trunking; Architecture and functional description (3GPP TS 24.525)".

[34] ETSI EN 300 899-1 (V1.1.2) (09-1998): "Integrated Services Digital Network (ISDN); Signalling System No.7; Interworking between ISDN User Part (ISUP) version 2 and Digital Subscriber Signalling System No. one (DSS1); Part 1: Protocol specification [ITU-T Recommendation Q.699, modified]".

[35] IETF RFC 7163: "URN for Country-Specific Emergency Services".

[36] draft-winterbottom-sipcore-locparam-01 (May 2017): "Location Source Parameter for the SIP Geolocation Header Field".

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI ES 282 001: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Functional Architecture".

[i.2] IETF RFC 3825: "Dynamic Host Configuration Protocol Option for Coordinate-based Location Configuration Information".

[i.3] IETF RFC 6225: "Dynamic Host Configuration Protocol Options for Coordinate-Based Location Configuration Information".

[i.4] ETSI TS 123 228: "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; IP Multimedia Subsystem (IMS); Stage 2 (3GPP TS 23.228)".

[i.5] ETSI TS 123 032: "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); Universal Geographical Area Description (GAD) (3GPP TS 23.032)".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

access network: portion of the telecommunications network that provides access to the switching function and terminates the user access signalling

Access Network Provider (ANP): service provider that provides physical and IP connectivity to a user equipment (UE) via a fixed or mobile access

NOTE: The access network may be provided by a single organization or it may be provided by a number of different organizations, BUT the interfaces between these organizations are not relevant to the scope of the present document as it is matter of contractual relations between the parties.

default PSAP: PSAP that is routed to when insufficient information exists to route to a specific PSAP, based on either location or emergency category

emergency: urgent need for assistance or relief

emergency call: call from a user to an emergency call centre, PSAP or similar agency charged with routeing calls to the relevant emergency response organization

emergency call facilities: mechanisms provided by public or private communications networks, emergency telephone stanchions/boxes, fire alarms, etc. the use of which enables emergency calls to be made

Emergency Call Service Provider (ECSP): service provider that acts as a mediator between the voice service providers and the public safety answering point service providers

emergency caller: individual placing an emergency call to reach the suitable PSAP

emergency category: differentiator for a specific emergency service type

NOTE: Examples of emergency service types are ambulance, police, fire brigade, etc.

emergency response organization: local or national force established to provide assistance to citizens in the event of their being involved in an emergency situation and requiring specialized help

EXAMPLE: The police, fire service and emergency medical services.

emergency service: service that provides immediate and rapid assistance in situations where there is a direct risk to life or limb, individual or public health or safety, to private or public property, or the environment but not necessarily limited to these situations

emergency situation: abnormal situation of serious nature that develops suddenly and unexpectedly, of which the evolution is uncertain and which may turn into a crisis or cause damage and casualties

Location-by-Reference: representing location information indirectly using a location URI

Location-by-Value: using location information in the form of a location object (LO), such as a PIDF-LO

location identifier: public network identifier, which provides a location value

EXAMPLE: A cell ID or line ID (see ETSI TS 123 167 [12]).

NOTE: A location value can be obtained from a location identifier by applying a static mapping or the location identifier may be encoded in such a way that it contains a location value (e.g. a ZIP code).

location information: location value, and/or a location identifier and/or a location reference

location reference: identifies a location server and provides sufficient information to allow the location server to provide the location value for the UE

EXAMPLE: https://ls.example.com:49152/uri/w3g61nf5n66p0, IETF RFC 6753 [25].

location URI: identifier that serves as a reference to location information which is later used as input by a dereference protocol to retrieve location information

location value: civic or geodetic position

network-provided location information: any location information pertaining to the calling device that is determined, provided or verified by the ANP

Next Generation Network (NGN): packet-based network able to provide telecommunication services and able to make use of multiple broadband, QoS-enabled transport technologies and in which service-related functions are independent from underlying transport-related technologies

nomadic: having the ability to move across network access points

NOTE: A nomadic user can make calls from different locations. However, unlike a mobile user, the location of a nomadic user cannot change during a specific call.

originating network: access network in which the emergency call was placed

PSAP address: URI or an E.164 number identifying a PSAP or a group of PSAPs

PSAP Service Provider (PSP): service provider that provides connectivity to Public Safety Answering Points (PSAPs) and directs emergency calls from the ECSP to the PSAP

Public Safety Answering Point (PSAP): physical location where emergency calls are received under the responsibility of a public authority

regulatory domain: geographical area where a set of regulatory rules applies

telecommunication: any transmission, emission, or reception of signs, signals, writing, images, sounds or intelligence of any nature, by wire, radio, optical fibre or other electromagnetic system

user access: point of connection to a telecommunication network from which a call can be placed

NOTE: This includes public telephones and "emergency call facilities".

user equipment: device allowing a user access to network services

user-provided location information: any location information originating from user-equipment that is not independently verified by the ANP

Voice Service Provider (VSP): specific type of application service provider that provides voice related services and optionally text and video-related services, on IP

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AF	Application Function
ANP	Access Network Provider
APRI	Address Presentation Restriction Indicator
AVP	Attribute-Value-Pair
CID	Content ID
CLF	Connectivity session Location and repository Function
DNS	Domain Name Server
EC	European Commission
E-CSCF	Emergency-Call Session Control Function
ECSP	Emergency Call Service Provider
ESRF	Emergency Service Routing Function
ESRP	Emergency Service Routeing Proxy
ETSI	European Telecommunications Standards Institute
EU	European Union
FQDN	Fully Qualified Domain Name
GAD	Universal Geographical Area Description
GMLC	Gateway Mobile Location Centre
HELD	HTTP Enabled Location Delivery
HTTPS	Hypertext Transfer Protocol Secure
IANA	Internet Assigned Numbers Authority
IBCF	Interconnection Border Control Function
IE	Information Element
IETF	Internet Engineering Task Force
II-NNI	Inter-IMS Network to Network Interface
IMS	IP Multimedia Core Network Subsystem
IP	Internet Protocol
ISUP	ISDN User Part
ITU-T	International Telecommunications Union - Telecommunications
LbyR	Location-by-Reference
LbyV	Location-by-Value
LRF	Location Retrieval Function
LS	Location Server
MLP	Mobile Location Protocol
NAPTR	Naming Authority PoinTeR
NGN	Next Generation Network
OMA	Open Mobile Alliance
P-CSCF	Proxy-Call Session Control Function
PSAP	Public Safety Answering Point
PSP	PSAP Service Provider
PSTN	Public Switched Telephone Network
RDF	Routeing Determination Function
RFC	Request For Comment
SIP	Session Initiation Protocol
SIPS	Session Initiation Protocol Secure
UA	User Agent
UE	User Equipment

URI	Uniform Resource Identifier
URL	Uniform Resource Locator
URN	Uniform Resource Name
VAE	VSP Aggregating Entity
VAP	VSP Aggregation Provider
VoIP	Voice over Internet Protocol
VSP	Voice Service Provider

4 Descriptions and assumptions

4.1 Introduction

ETSI ES 203 178 [1] defines the interfaces between functional entities in the functional architecture to support European requirements on emergency caller location determination and transport, and places requirements on each of these interfaces. However, it does not specify what protocols are available or might be used to implement the required functionality across each of the interfaces. The present document matches interfaces with existing protocols and where gaps exist clearly indicates what the gaps are.

Table 4.1 summarizes the interfaces defined in ETSI ES 203 178 [1] and categorizes them as being either in scope or out of scope for the present document. Interfaces deemed as "In Scope" have specific clauses detailing how to achieve the functionality specified in ETSI ES 203 178 [1]. The details may refer to other specification, profile or extend existing protocols, or define new protocols. Interfaces deemed "Out of Scope" do not have detailed specifications provided in the present document.

Table 4.1: Categories of Interfaces defined in ETSI ES 203 178 [1]

Interface	1st endpoint	2nd endpoint	Scope
ia	User equipment	VSP Call Control	Out of scope
ib	VSP Call Control	LS Discovery	In scope
ic	VSP Call Control	Location Server	In scope
id	Location Server	Route Server	In scope
ie	VSP Call Control/VAE	VAE/ESRF	In scope
if	ESRF/LS-Proxy	Location Server	In scope
ig	ESRF	Route Server	In scope
ih	ESRF	ESRP	In scope
ii	ESRP	PSTN-PSAP	In scope
ij	ESRP	IP-PSAP	In scope
ik	PSTN-PSAP	ESRF/LS-Proxy	In scope
il	IP-PSAP	Location Server	In scope
im	IP-PSAP	ESRF/LS-Proxy	In scope
in	ESRF	LS-Proxy	In scope

As is stated in ETSI ES 203 178 [1], some interfaces in the architecture are between functional entities belonging to different operators or providers and, as a consequence, these interfaces have interoperability requirements and shall be implemented following the present document by the related connected functional entities. The protocol selection for these interfaces can impose requirements on provider internal functionalities and some provider internal interfaces; the definition of these requirements is however outside the scope of the present document.

The EC standardisation mandate M/493 (see ETSI ES 203 178 [1], annex B) demands that "this work shall not be focused on NGN but shall address current implementations for all types of voice calls (fixed, mobile, static and nomadic VoIP) in EU countries". Consequently, the functional architecture is intended to be compatible with IMS-based deployments and specifications regarding emergency services provision. The present document includes statements on IMS/NGN implementation considerations per interface.

IMS considerations can include statements regarding the IMS protocol assignment, parameterization and control plane interworking.

The interfaces ia, ib, ic and ie are external, which means between country A and anywhere and (with the exception of ia) are specified in detail to ensure that all VSPs and VAPs can participate in the processes for emergency service caller location determination and transport based on the architecture of ETSI ES 203 178 [1] within country A.

The interfaces id, if, ig, ih, ii, ij, ik, il, im and in are internal, inside country A, and should be specified considering the existing national implementations and regulations in country A. When other protocols are used care is to be taken that all information elements outlined in the architecture are covered.

5 Protocol specifications for the interfaces of the functional architecture in ETSI ES 203 178

5.1 Interface ia

The protocol used on the interface ia is determined by the VSP only and is therefore out of scope for the present document.

5.2 Interface ib

5.2.1 Protocol specifications

The ib interface defines the interactions between the VSP call control and the LS discovery functional entity. The VSP call control uses the public IP address of the UE to interrogate the LS discovery functional entity in order to obtain the address of the LS serving the access network to which the UE is attached. Since this function is expected to be accessible to any VSP anywhere, this is an open interface.

If a pre-established relationship exists between the ANP and the VSP then DNS may be used for the LS discovery function. The first part of this discovery process in IETF RFC 7216 [19] yields the domain name of the serving access network. If the VSP knows the address of the LS for the serving ANP, then no further discovery is required, otherwise an additional DNS query may be used.

If no pre-established relationship exists between the VSP and the ANP then the LS Discovery function shall use the Domain Name Service (DNS). The VSP requires the URL of the LS serving the access network to which the UE is attached. The URL shall be a HELD URI (IETF RFC 5985 [20]). The URL discovery shall perform the U-NAPTR procedures defined in sections 2 and 4 of IETF RFC 5986 [21] with the following variations:

- the domain shall be known as a result of having performed the steps in IETF RFC 7216 [19]; and
- the device based interfaces are irrelevant as discovery is performed by a third-party, i.e. the VSP; and
- the process stops once the URL for the LS has been resolved based on the steps in section 4 of IETF RFC 5986 [21].

5.2.2 IMS/NGN implementation considerations

This interface is between the VSP call control and the LS Discovery functionality.

This interface is not part of the IMS architecture as specified in ETSI TS 123 228 [i.4] and it is not part of the NGN architecture as specified in ETSI ES 282 001 [i.1].

5.3 Interface ic

5.3.1 Protocol specifications

5.3.1.1 General

Depending on the pre-established relationship the VSP call control can use interface ic to request location and routeing information from the location server. The following clauses differentiate cases where a pre-established relationship between entities exists or not.

When the ANP trusts the VSP, and the VSP has been given knowledge of this trust by prior agreement, then clauses 5.3.1.3 or 5.3.1.4 can be used to request location. Clause 5.3.1.4 can only be used when the ANP provides a gateway mobile location centre (GMLC).

Otherwise clause 5.3.1.2 shall be used.

5.3.1.2 Location request without pre-established relationship between VSP and ANP

Where no pre-established relationship exists between the VSP and the ANP then the HELD protocol (IETF RFC 5985 [20]) shall be used by the VSP to acquire location from the LS. The VSP shall use IP address and port information in the HELD request to the LS using HELD device identity extensions defined in IETF RFC 6155 [22]. Where the VSP has the full IP flow identity information available then it shall use the IP flow identity definitions in IETF RFC 6915 [23]. The VSP shall set:

- the locationType to "any"; and
- the exact attribute to "false"; and
- the responseTime to "emergencyRouting".

The VSP includes a request for routeing information as described in IETF RFC 7840 [24]. The VSP shall not set the service attribute in the routeing request unless the UE has identified a specific service to the VSP over ia. If the service attribute is set then its value shall be identical to the value provided by the UE.

If the LS has no pre-established relationship with the VSP then the LS shall not return a location value but shall return a location reference in the form of a location URI using the HTTPS URI schemes.

If the HELD request to the LS includes request for routeing information then the LS shall provide routeing information in accordance with IETF RFC 7840 [24] in the location response message.

NOTE: The HELD protocol does not define explicitly the transport of location identifiers as specified in ETSI ES 203 178 [1]. In order for HELD to convey these items without modification, location identifiers would need to be encoded as some kind of URI.

Tables 5.1 and 5.2 describe the elements used for the HELD location request and location response via the ic interface.

In table 5.1 column 1 represents the element name of the HELD protocol. Column 2 indicates the status of this element (mandatory, conditional or optional). Column 3 describes additional requirements and the mapping of the element to the information element (IE) in ETSI ES 203 178 [1]. Column 4 specifies the permitted values for the element in column 1.

Table 5.1: HELD Location Request

HELD Element Name	Status in HELD	Description and related ETSI ES 203 178 [1] Information element with (Status in ETSI ES 203 178 [1])	Value
responseTime	M	The time in which the requesting entity would like a response in ms. LS defined values for emergencyRouting and emergencyDispatch can also be used Not defined in ETSI ES 203 178 [1].	emergencyRouting
requestRoutingInformation	M	Allows the requesting entity to request routing information ETSI ES 203 178 [1]: Routing request (O).	Empty or urn:service:sos or urn:servive:sos with a subtype
locationType	M	Specifies the form that the requesting entity would like the location to come in. Not defined in ETSI ES 203 178 [1].	any
exact	M	Specifies whether the server returns an error if the requested locationType is not available. Not defined in ETSI ES 203 178 [1].	false
device	C	The VSP call control shall provide a device identifier to specify IP address and port if a complete IP flow is not available. The VSP call control may include device identity information in addition to the complete IP flow being available. The structure and format of device identifiers shall comply with the provisions in IETF RFC 6155 [22]. The LS shall only use the device information if it is unable to identify the device based on flow information.	IP address (+ port)
flow	C	The VSP call control shall provide the IP flow between the source and destination if available as specified in IETF RFC 6915 [23]. The LS shall try to determine the location of the device using the full IP flow information if possible. The LS may use information provided in the device element if IP flow information is not provided or is insufficient to allow device location to be determined. ETSI ES 203 178 [1]: Calling IP address and port (M).	Source IP address + port and Destination IP address + port

In table 5.2 column 1 represents the element name of the HELD protocol. Column 2 indicates the status of this element (mandatory, conditional or optional). Column 3 describes additional requirements and the mapping of the element to the information element (IE) in ETSI ES 203 178 [1]. Column 4 specifies the permitted values for the element in column 1.

Table 5.2: HELD Location Response

HELD Element Name	Status in HELD	Description and related ETSI ES 203 178 [1] Information element with (Status in ETSI ES 203 178 [1])	Value
locationUriSet	C	If the location response from the location server has either a location reference or a location identifier to return the locationUriSet parameter shall be present in the response. ETSI ES 203 178 [1]: Network-provided location information (M)	locationURI, expires
Presence	C	If the location server needs to return a location value, either civic, geodetic or both, then the Presence element shall be present. ETSI ES 203 178 [1]: Network-provided location information (M)	Location-info (PIDF-LO)
routingInformation	C	If the locationRequest included a requestRoutingInformation attribute, then the response shall contain routingInformation ETSI ES 203 178 [1]: ESRF URI (C)	<service serviceUri="urn:service:sos"> <dest>sip:112@example.com</dest> (and <dest>sips:112@example.com</dest>) <dest>xmpp:112@example.com</dest> </service> (see note)
NOTE: For the dest field, a SIP URI shall be used. A SIPS URI may be used in addition to the SIP URI. If the VSP is able to route the SIPS URI destination, then the SIPS URI should be used to enhance security.			

5.3.1.3 Location request in the case of pre-established relationship between VSP and ANP

When the ANP trusts the VSP, and the VSP has been given knowledge of this trust by prior agreement the protocol defined in ETSI ES 283 035 [13] may be used between the VSP and the LS as an alternative to the HELD protocol (IETF RFC 5985 [20]). In case the HELD protocol is used, tables 5.1 and 5.2 apply with the exception that the LS can return a location value.

NOTE: No explicit LS discovery mechanism exists for this option so the relationship between the entities needs to include how the VSP identifies the corresponding LS.

ETSI ES 283 035 [13] specifies a Diameter application between an Application Function (AF) and a Connectivity session Location and repository Function (CLF). An AF sends an "Information Query Request" message to a CLF. In IMS, the AF may be a P-CSCF that performs the functions of the VSP call control in the ETSI ES 203 178 [1] functional architecture. Similarly, the CLF can provide the LS functions.

In table 5.3 column 1 represents the information element name of the "Information Query Request". Column 2 indicates the mapping to the diameter AVP. Column 3 indicates the category of this Diameter element (mandatory, conditional or optional). Column 4 provides information and defines the mapping of the Diameter protocol element to the information element (IE) in ETSI ES 203 178 [1].

Table 5.3: Information Query Request

Information element name in ETSI ES 283 035 [13]	Mapping to diameter AVP	Cat. in ETSI ES 283 035 [13]	Description and related ETSI ES 203 178 [1] Information element with (Status in ETSI ES 203 178 [1])
Globally unique IP Address	Globally-Unique-Address	C	This information element contains: • The IP address of the UE for which the profile information is being requested • The addressing domain in which the IP address is significant ETSI ES 203 178 [1]: Calling IP address and Port (part of) (M). See note 2.
IP Connectivity User ID	User-Name	C	The identity of the IP connectivityuser that is attached to the network. Not defined in ETSI ES 203 178 [1].
Access Identifier	Global-Access-Id	C	Identifies an access point to IP connectivity services. ETSI ES 203 178 [1]: Location identifier (O).
AF Identity	AF-Application-Identifier	M	Identifies the AF originating the request Not defined in ETSI ES 203 178 [1]. This parameter shall be set to the VSP call server identity.
Requested-Items	Requested-Information	O	The list of items requested by the AF. This parameter shall be set to LOCATION-INFORMATION (1) and EMERGENCY-CALL-ROUTING-INFO (11) if routeing information is requested. ETSI ES 203 178 [1]: Routeing Request (O).
Port-Number	Port-Number	C	The originating port number associated to the session for which the AF is attempting to retrieve information. ETSI ES 203 178 [1]: Calling IP address and port (part of) (M). See note 3.
NOTE 1: Either the Globally-Unique-IP-Address and the Port-Number or the IP connectivity user ID or the Access Identifier shall be included. NOTE 2: Port information is provided in a separate parameter. NOTE 3: This parameter shall be included when the Globally unique IP address is used in a request.			

The CLF responds to the "Information Query Request" with an "Information Query Response" to the AF.

In table 5.4 column 1 represents the information element name of the "Information Query Response". Column 2 indicates the mapping to the diameter AVP. Column 3 indicates the category of this Diameter element (mandatory, conditional or optional). Column 4 provides information and defines the mapping of the Diameter protocol element to the information element (IE) in ETSI ES 203 178 [1].

Table 5.4: Information Query Response

Information element name in ETSI ES 203 178 [1]	Mapping to diameter AVP	Cat. in ETSI ES 283 035 [13]	Description and related ETSI ES 203 178 [1] Information element with (Status in ETSI ES 203 178 [1])
Result	Result-Code/Experimental-Result	M	Result of the request.
Location Information	Location-Information	O	Location information (or a pointer to such information) in a form that is suitable for the requesting application. ETSI ES 283 035 [13] provides four types of location information: - Line-Identifier, - Civic-Location, -Geospatial-Location and - PIDF-LO. ETSI ES 203 178 [1]: Network-provided location information (M). See note 1. The only pointer-type information currently defined in the AVP however is the Line-Identifier, which is a location identifier in ETSI ES 203 178 [1]. ETSI ES 283 035 [13] does not support location by reference.
Physical Access ID	Physical-Access-Id	O	The identity of the physical access where the user equipment is connected.
Emergency-Call-Routeing-Info	Emergency-Call-Routeing-Info	C	An URI where to route emergency calls originated from the access and/or session considered. See note 2.
NOTE 1: The Geospatial-Location element constrains the location format to that used in IETF RFC 3825 [i.2], which has subsequently been corrected by IETF RFC 6225 [i.3], but even so it does not provide sufficient range to address the shape types typically used by cellular network and specified in 3GPP GAD standard ETSI TS 123 032 [i.5]. NOTE 2: Considering ETSI ES 203 178 [1] requirements the LS shall provide an Emergency-Call-Routeing-Info AVP if required in the Information-Query-Request.			

5.3.1.4 Location request to a gateway mobile location centre

Cellular networks as specified by 3GPP define the gateway mobile location centre (GMLC) as their location server. The application protocol specified for querying a GMLC is the Open Mobile Alliance's (OMA) mobile location protocol (MLP) [2]. There are currently no Application Protocol Tags or Application Service Tags defined in the IANA registries to enable discovery of the correct GMLC so this function would need to be covered by the relationship between the VSP and ANP.

NOTE As MLP does not support the provision of routing information no further details on this protocol option are provided with the present document.

5.3.2 IMS implementation considerations

This interface is used by the VSP call control to request location and routeing information from the location server.

For routing information retrieval:

This is not an IMS reference point.

If the VSP is IMS-based, there is no need for retrieving routeing information from an external server (the P-CSCF determines the E-CSCF address as specified in ETSI TS 124 229 [10]).

For location information retrieval:

This is not an IMS reference point.

If the VSP is IMS-based and the ANP is a wireline network, the solution specified in ETSI ES 283 035 [13] for the interface between a P-CSCF and a CLF applies.

NOTE: If the VSP is IMS-based and the ANP is a wireless access network, the applicability of the above solution is not covered in the present document.

5.4 Interface id

5.4.1 Protocol specifications

Interface id can be used by the location server to acquire routeing information from the route server. Interface id can be an intra-operator or an inter-operator interface. Often, the routeing information can be determined at the time that location information is provisioned into the LS. Other implementations may allow the LS to be provisioned with location information, and then require the LS to "validate" the provisioned location information against the route server, to ensure that the location information is in the correct format.

Standardisation of this interface is not covered in the present document. The access to a route server for emergency calls is a matter of national regulation.

5.4.2 IMS implementation considerations

This interface is between the Location Server and the Route server and it is used by the LS to acquire routing information.

This is not an IMS reference point.

5.5 Interface ie

5.5.1 Protocol specifications

The interface ie interacts between the VSP call control and the ESRF in the ECSP network. In the case where a VSP is connected via a VAP, the interface ie defines the interactions between the VSP call control and the VAE and between the VAE and the ESRF. This is an open interface, all VSPs, VAPs and ECSPs shall provide this interface.

Entities at each end of the interface shall support the following specifications as appropriate for either proxy or UA usage:

- IETF RFC 3261 [3].
- IETF RFC 4320 [4].
- IETF RFC 5393 [5].
- IETF RFC 5954 [6].
- IETF RFC 6442 [7].
- IETF RFC 4566 [8].
- IETF RFC 3264 [9].

The VSP call control and the VAE shall use the Session Initiation Protocol (SIP) towards the ESRF. Table 5.5 describes the mapping between information elements defined in ETSI ES 203 178 [1] to be conveyed across the ie interface and the specifications containing the relevant SIP header fields.

In table 5.5 column 1 represents the Information Element (IE) in ETSI ES 203 178 [1]. Column 2 lists the relevant specifications, for which normative requirements are described in column 4. Column 3 specifies the header fields in SIP that maps to this IE in ETSI ES 203 178 [1]. Column 4 contains requirements and additional information.

Table 5.5: SIP interface ie

IE	Specifications	SIP header field	Requirements and additional information
Called Identity	IETF RFC 5031 [26], IETF RFC 6881 [27]	Request URI = urn:service:sos Including subservice types	This is commonly accepted as the means to mark an emergency call in SIP. There are specific service types for police, fire and ambulance as well as other emergency responder types specified in IETF RFC 5031 [26], so the specific service type may be requested. If the specific service type requested is not available then top-most service urn or urn:service:sos may be used. Some countries have emergency service entities that are specific to them. IETF RFC 7163 [35] specifies how these can be defined and used. Request URI contains only service URNs If the VSP receives dialled digits it shall performs digit analysis and converts it to service URN (in accordance with proxy role of IETF RFC 6881 [27]) unless an agreement between the VSP and the ECSP allows the transmission of dialled digits or national regulation in country A requires it. The VSP should pass on all service URN subtypes it receives even if it is not supported in the regulatory regime of the VSP (IETF RFC 5031 [26]). Emergency test call facilities, such as those outlined in IETF RFC 6881 [27], are outside of the scope of the present document. A VSP shall not pass on any emergency call where the user-provided service URN is urn:service:test:sos or any associated subtypes.
Network-provided caller identity	IETF RFC 3325 [28] IETF RFC 3323 [30] IETF RFC 5079 [31]	P-Asserted-Identity	This header field contains the identity of the caller and is inserted by a trusted proxy, in ETSI ES 203 178 [1] this is the VSP call control. P-Asserted-Identity is using a non-cryptographic method based on a so called chain-of-trust. The transmission of a trusted identity in the P-Asserted-Identity header field is mandatory in the case of a trust relationship between interconnected networks. The originating network shall ensure that the subscriber's information in the P-Asserted Identity header field (both user part and host portion) are verified, screened and hence can uniquely be assigned to a certain subscriber. The P-Asserted-Identity header field shall be set up by the originating network operator and shall be transmitted transparently through the networks. See note. A Privacy header field with the values "id" and/or "header" may appear in accordance with IETF RFC 3323 [30], and the additional requirements contained within IETF RFC 3325 [28]. If the VSP does not send the P-Asserted caller identity the ECSP shall, depending on national regulation in country A, either respond to the INVITE request with a request failure code 433 (Anonymity Disallowed) as defined in IETF RFC 5079 [31] or proceed with the call establishment without the network-provided caller identity.

IE	Specifications	SIP header field	Requirements and additional information
Network-provided location information	IETF RFC 6442 [7] IETF RFC 4119 [15] IETF RFC 5139 [16] IETF RFC 5491 [17] IETF RFC 6848 [18]	Geolocation	The Geolocation header field indicates that the SIP message, in this case an INVITE, contains either a location value or a location URI depending on the value in the header. The SIP Geolocation Header field is defined in IETF RFC 6442 [7]. IETF RFC 4119 [15] defines so called Presence Information Data Format - Location Objects (PIDF-LO) which are used by IETF RFC 6442 [7]. Further PIDF-LO types are defined by IETF RFC 5139 [16]. General information on how to constrain, represent, and interpret locations in a PIDF-LO are described in IETF RFC 5491 [17]. IETF RFC 6848 [18] describes how new civic address elements are added. ETSI ES 203 178 [1] supports multiple location sources adding location to the call. Location ordering as defined in IETF RFC 6442 [7] applies. Location information may be location-by-value in the form of a PIDF-LO contained in the body of the SIP INVITE message, or a location reference in the form of a location URI conforming to the HTTP(S) or SIP(S) URI schemes. In addition to ordering it is necessary to know the identity of the entity adding location information to the call so that downstream entities can decide in which provider of location they have more confidence. This accomplished using the loc-src parameter defined in draft-winterbottom-sipcore-locparam-01 [36].
User-provided caller identity	IETF RFC 3261 [3]	From	The identity of the UE conveyed over ia is mapped to the SIP From header field by the VSP. If the protocol at the ia reference point is SIP, then the value in the From header field is copied from ia to ie. If no user-provided caller identity is provided the VSP shall select a value consistent with that used in the network-provided caller identity. In case of multiple identities are received by the VSP the selection of the most appropriate is outside of the scope of the present document.
User-provided location information	IETF RFC 6442 [7] IETF RFC 4119 [15] IETF RFC 5139 [16] IETF RFC 5491 [17] IETF RFC 6848 [18]	Geolocation Geolocation-Routing	The Geolocation header field indicates that the SIP message, in this case an INVITE, contains either a location value or a location URI depending on the value in the header. The SIP Geolocation Header field is defined in IETF RFC 6442 [7]. IETF RFC 4119 [15] defines so called Presence Information Data Format - Location Objects (PIDF-LO) which are used by IETF RFC 6442 [7]. Further PIDF-LO types are defined by IETF RFC 5139 [16]. General information on how to constrain, represent, and interpret locations in a PIDF-LO are described in IETF RFC 5491 [17]. IETF RFC 6848 [18] describes how new civic address elements are added. The Geolocation-Routing header field explicitly grants permission for the location information to be used for routing. The values are comma separated in the same Geolocation header field. Provision has been made for each location value to have a generic-param defined, but does not currently define any parameters.

IE	Specifications	SIP header field	Requirements and additional information
			ETSI ES 203 178 [1] supports multiple location sources adding location to the call. Location ordering as defined in IETF RFC 6442 [7] applies. Location information may be location-by-value in the form of a PIDF-LO contained in the body of the SIP INVITE message, or a location reference in the form of a location URI conforming to the HTTP(S) or SIP(S) URI schemes. In addition to ordering it is necessary to know the identity of the entity adding location information to the call so that downstream entities can decide in which provider of location they have more confidence. This accomplished using the loc-src parameter defined in draft-winterbottom-sipcore-locparam-01 [36].
IP address and port	IETF RFC 3261 [3]	Via	Where known by the UE it should include its public IP address and identifying port in the Via header field. The bottommost Via header field added by the UE contains the IP address and port of the UE. UE IP address and port information is used to determine the LS and acquire location and routeing information. If location and routeing information is provided in the SIP INVITE message then UE IP address and port information need not be passed over interface ie.
VAP URI	IETF RFC 3261 [3]	Route	In the case when the emergency call is routed via a VAP the VSP Call Control insert a Route header field. The URI in the Route header field will be provided in advance by the VAP to the VSP as a valid URI to address a VAE resource.
VSP identity	IETF RFC 7852 [29]	ProviderInfo	This element shall be supplied by the VSP and is either a MIME component in the body of the SIP INVITE or a data field stored on an external repository. The VSP shall include in the SIP Call-Info header field of the SIP INVITE a URI pointing to the ProviderInfo. In the first case, the URI in the Call-Info-header is a CID URI, in the second case it is a pointer (e.g. a HTTPS URI) which can be dereferenced by authorized third parties (e.g. a PSAP); these cases are both specified in IETF RFC 7852 [29]. The ProviderInfo includes the following data elements, and the VSP shall include all these elements with appropriate information, in accordance with IETF RFC 7852 [29]: • DataProviderReference. • DataProviderString. • ProviderID. • ProviderIDSeries. • TypeOfProvider: Value "Telecom Provider". • Language. • DataProviderContact. • Any VAP shall pass the VSP identity without modification.
NOTE: The VSP can pass on any received Identity header field independent of usage of P-Asserted-Identity.			

5.5.2 IMS implementation considerations

In the case where the VSP and ECSP are both IMS but are run by different operators then Inter-IMS Network to Network Interface protocol, as specified in ETSI TS 129 165 [11], applies.

The interface Ici of ETSI TS 129 165 [11] conforms to the interface ie.

In the context of the present document, the non-roaming II-NNI traversal scenario (originating home network - terminating home network) applies to the interface ie.

Location-based information shall be exchanged according to clause 5.5.1 of the present document.

In the case where the VSP and the ECSP are both IMS and are run by the same operator the interface ie becomes an internal interface and ETSI TS 124 229 [10] applies, as specified for the interface at the Mw reference point.

If the VSP has deployed a SIP-based IP network and the ECSP is a different operator with IMS or vice versa, the VSP shall appear to the ECSP as if it were an IBCF complying with the requirements identified in ETSI TS 124 229 [10], clause 4.1 for this functional entity. When processing an emergency call, IBCF implementations are expected to be transparent to unrecognized information unless specific exceptions exist.

Location-based information shall be exchanged according clause 5.5.1 of the present document.

5.6 Interface if

5.6.1 Protocol specifications

The if interface defines the interactions between the LS and the LS Proxy. If no LS proxy acts between the ESRF and the LS, the if interface coincides with the in interface.

Option 1

Upon receipt of a location reference in form of a location URI the ESRF shall initiate location dereferencing according to the IETF HELD dereference specification IETF RFC 6753 [25].

If the locationURI is available, tables 5.6 and 5.7 describe the elements used for the HELD location request and location response via the if interface.

In table 5.6 column 1 represents the element name of the HELD protocol. Column 2 indicates the status of this element (mandatory, conditional or optional). Column 3 describes additional requirements and the mapping of the element to the information element (IE) in ETSI ES 203 178 [1]. Column 4 specifies the permitted values for the element in column 1.

Table 5.6: HELD Location Request based on a locationURI

HELD Element Name	Status in HELD	Description and related ETSI ES 203 178 [1] Information element with (Status in ETSI ES 203 178 [1])	Value
responseTime	M	The time in which the requesting entity would like a response in ms. Not defined in ETSI ES 203 178 [1].	If the ESRF/LS-Proxy is requesting location information for the purposes of routing the call to the PSAP then it shall set the responseTime in the HELD locationRequest to "emergencyRouting". If the ESRF/LS-Proxy is requesting location information on behalf of the PSAP to assist with dispatching emergency crews then the responseTime in the HELD locationRequest shall be set to "emergencyDispatch"
locationType	M	Specifies the form that the requesting entity would like the location to come in. Not defined in ETSI ES 203 178 [1].	civic or geodetic
exact	M	Specifies whether the server returns an error if the requested locationType is not available. Not defined in ETSI ES 203 178 [1].	False
locationURI	M	URI to be used to retrieve a location value.	locationURI, expires

HELD Element Name	Status in HELD	Description and related ETSI ES 203 178 [1] Information element with (Status in ETSI ES 203 178 [1])	Value
		Either location reference or location identifier shall be included. ETSI ES 203 178 [1]: location reference (C), location identifier (C).	

In table 5.7 column 1 represents the element name of the HELD protocol. Column 2 indicates the status of this element (mandatory, conditional or optional). Column 3 describes additional requirements and the mapping of the element to the information element (IE) in ETSI ES 203 178 [1]. Column 4 specifies the permitted values for the element in column 1.

Table 5.7: HELD Location Response based on a locationURI

HELD Element Name	Status in HELD	Description and related ETSI ES 203 178 [1] Information element with (Status in ETSI ES 203 178 [1])	Value
Presence	M	The location server shall return a location value, either civic, geodetic or both. ETSI ES 203 178 [1]: location value (M).	Location-info (PIDF-LO)

If a location reference or a location identifier is not available the ESRF or the LS Proxy can initiate location dereferencing according to the IETF specification IETF RFC 6155 [22] using a device identifier. Tables 5.8 and 5.9 describe the elements used for the location request and location response based on a device identifier via the if interface.

In table 5.8 column 1 represents the element name of the HELD protocol. Column 2 indicates the status of this element (mandatory, conditional or optional). Column 3 describes additional requirements and the mapping of the element to the information element (IE) in ETSI ES 203 178 [1]. Column 4 specifies the permitted values for the element in column 1.

Table 5.8: HELD Location Request based on a device identifier

HELD Element Name	Status in HELD	Description and the related ETSI ES 203 178 [1] Information element with (Status in ETSI ES 203 178 [1])	Value
responseTime	M	The time in which the requesting entity would like a response in ms. LS defined values for emergencyRouting and emergencyDispatch can also be used Not defined in ETSI ES 203 178 [1].	If the ESRF/LS-Proxy is requesting location information for the purposes of routing the call to the PSAP then it shall set the responseTime in the HELD locationRequest to "emergencyRouting". If the ESRF/LS-Proxy is requesting location information on behalf of the PSAP to assist with dispatching emergency crews then the responseTime in the HELD locationRequest shall be set to "emergencyDispatch"
locationType	M	Specifies the form that the requesting entity would like the location to come in. Not defined in ETSI ES 203 178 [1].	civic or geodetic
exact	M	Specifies whether the server returns an error if the requested locationType is not available. Not defined in ETSI ES 203 178 [1].	False
device	M	The ESRF/LS Proxy shall provide a device identifier to specify IP address and port or other device identifiers defined in IETF RFC 6155 [22]. ETSI ES 203 178 [1]: Calling IP address and port (O).	IP address (+ port) or other device identifier according to IETF RFC 6155 [22]

In table 5.9 column 1 represents the element name of the HELD protocol. Column 2 indicates the status of this element (mandatory, conditional or optional). Column 3 describes additional requirements and the mapping of the element to the information element (IE) in ETSI ES 203 178 [1]. Column 4 specifies the permitted values for the element in column 1.

Table 5.9: HELD Location Response based on a device identifier

HELD Element Name	Status in HELD	Description and related ETSI ES 203 178 [1] Information element with (Status in ETSI ES 203 178 [1])	Value
Presence	C	The location server can return a location value, either civic, geodetic or both (see note). ETSI ES 203 178 [1]: Location value (M).	Location-info (PIDF-LO)
locationURI	C	URI to be used as a pointer to a location value (see note). Either location reference or location identifier shall be included. ETSI ES 203 178 [1]: Location reference (C), Location identifier (C).	locationURI, expires
NOTE: One of these location elements shall be included.			

Option 2

Depending national regulation the Open Mobile Alliance (OMA) Mobile Location Protocol (MLP) Version 3.5 [2] may be used.

NOTE: As MLP does not support the provision of routing information no further details on this protocol option are provided with the present document.

5.6.2 IMS/NGN implementation considerations

This is the interface between the ESRF/LS-Proxy and the Location Server.

This interface is not part of the IMS architecture as specified in ETSI TS 123 228 [i.4] and it is not part of the NGN architecture as specified in ETSI ES 282 001 [i.1].

It can be a web service-based interface, identical to the interface "il".

5.7 Interface ig

5.7.1 Protocol specifications

Interface ig can be used by the ESRF to acquire routeing information from the route server. Interface ig can be an intra-operator or an inter-operator interface. Often, the routeing information can be determined at the time that location information is provisioned into the ESRF.

In addition, the route server can provide a PSTN-PSAP URI or FQDN as location push destination in the case that the location information is pushed via interface ik.

Standardisation of this interface is not covered in the present document. The access to a route server for emergency calls is a matter of national regulation.

5.7.2 IMS implementation considerations

This is the interface between the ESRF and the Route Server. In IMS implementations the E-CSCF can get routing information through the Ml reference point, through the Location Retrieval Function LRF, as specified in ETSI TS 124 229 [10]. ETSI TS 123 167 [12] defines configurations where the LRF consists of a Routing Determination Function (RDF) and a LS. The interface between Location Server and RDF is out of scope of ETSI TS 123 167 [12]. In this context, interface ig does not relate to an IMS reference point.

5.8 Interface ih

5.8.1 Protocol specifications

The interface ih is located between the ESRF and the ESRP. According to ETSI ES 203 178 [1], this is an internal interface inside country A. If the interface ih is IP-based and SIP is used across this interface, table 5.10 describes the mapping between information elements defined in ETSI ES 203 178 [1] to be conveyed across the ih interface and the specifications containing the relevant SIP header fields.

In table 5.10 column 1 represents the Information Element (IE) in ETSI ES 203 178 [1]. Column 2 lists the relevant specifications, for which normative requirements are described in column 4. Column 3 specifies the header fields in SIP that maps to this IE in ETSI ES 203 178 [1]. Column 4 contains requirements and additional information.

Table 5.10: ih interface SIP case

IE	Specifications	SIP header field	Requirements and additional information
Called Identity	IETF RFC 3261 [3] IETF RFC 6881 [27]	Request URI or Route header field (see note)	The PSAP address is determined by the ESRF in the context of national requirements applicable to emergency services.
Network-provided caller identity	IETF RFC 3325 [28]	P-Asserted-Identity	If the VSP sends a P-Asserted caller identity, the ESRF shall pass it transparently.
Network-provided location information	IETF RFC 6442 [7] IETF RFC 4119 [15] IETF RFC 5139 [16] IETF RFC 5491 [17] IETF RFC 6848 [18]	Geolocation	The Geolocation header field indicates that the SIP message, in this case an INVITE, contains either a location value or a location URI depending on the value in the header. The SIP Geolocation Header field is defined in IETF RFC 6442 [7]. IETF RFC 4119 [15] defines so called Presence Information Data Format - Location Objects (PIDF-LO) which are used by IETF RFC 6442 [7]. Further PIDF-LO types are defined by IETF RFC 5139 [16]. General information on how to constrain, represent, and interpret locations in a PIDF-LO are described in IETF RFC 5491 [17]. IETF RFC 6848 describes how new civic address elements are added [18]. ETSI ES 203 178 supports multiple location sources adding location to the call. Location ordering as defined in IETF RFC 6442 [7] applies. Location information may be location-by-value in the form of a PIDF-LO contained in the body of the SIP INVITE message, or a location reference in the form of a location URI conforming to the HTTP(S) or SIP(S) URI schemes. In addition to ordering it is necessary to know the identity of the entity adding location information to the call so that downstream entities can decide in which provider of location they have more confidence. This accomplished using the loc-src parameter defined in draft-winterbottom-sipcore-locparam-01 [36].
User-provided caller identity	IETF RFC 3261 [3]	From	The identity of the UE conveyed over ia is mapped to the SIP From header field by the VSP. The value in the From header field is copied from ie to ih.
User-provided location information	IETF RFC 6442 [7] IETF RFC 4119 [15] IETF RFC 5139 [16] IETF RFC 5491 [17] IETF RFC 6848 [18]	Geolocation Geolocation-Routing	The Geolocation header field indicates that the SIP message, in this case an INVITE, contains either a location value or a location URI depending on the value in the header. The SIP Geolocation Header field is defined in IETF RFC 6442 [7]. IETF RFC 4119 [15] defines so called Presence Information Data Format - Location Objects (PIDF-LO) which are used by IETF RFC 6442 [7]. Further PIDF-LO types are defined by IETF RFC 5139 [16]. General information on how to constrain, represent, and interpret locations in a PIDF-LO are described in IETF RFC 5491 [17]. IETF RFC 6848 describes how new civic address elements are added [18].

IE	Specifications	SIP header field	Requirements and additional information
			The Geolocation-Routing header field explicitly grants permission for the location information to be used for routing. The values are comma separated in the same Geolocation header field. Provision has been made for each location value to have a generic-param defined, but does not currently define any parameters. ETSI ES 203 178 supports multiple location sources adding location to the call. Location ordering as defined in IETF RFC 6442 [7] applies. Location information may be location-by-value in the form of a PIDF-LO contained in the body of the SIP INVITE message, or a location reference in the form of a location URI conforming to the HTTP(S) or SIP(S) URI schemes. In addition to ordering it is necessary to know the identity of the entity adding location information to the call so that downstream entities can decide in which provider of location they have more confidence. This accomplished using the loc-src parameter defined in draft-winterbottom-sipcore-locparam-01 [36].
IP address and port	IETF RFC 3261 [3]	Via	The value in the Via header field is copied from ie to ih, if received via the ie interface. The bottommost Via header field added by the UE contains the IP address and port of the UE.
VSP identity	IETF RFC 7852 [29]	ProviderInfo	The VSP identity is either a MIME component in the body of the SIP INVITE or a data field stored on an external repository. The SIP Call-Info header field of the SIP INVITE contains a URI pointing to the ProviderInfo. In the first case, the URI in the Call-Info-header is a CID URI, in the second case it is a pointer (e.g. a HTTPS URI) which can be dereferenced by authorized third parties (e.g. a PSAP). The ProviderInfo includes the following data elements: DataProviderReference DataProviderString ProviderID ProviderIDSeries TypeOfProvider: Value "Telecom Provider" Language DataProviderContact This element need not be passed via the interface ih if national regulation does not require it, or if the identity can be inferred from the Network-provided caller identity. If the VSP identity is passed on, than the ECSP shall pass on the VSP identity as received, without modification.
NOTE: When the Called Identity is mapped to the Route header field, the Request URI shall contain the original Service URN. When the Called Identity is mapped to the Request URI it shall contain a SIP URI or a telURI. The choice between the two mapping options is a national matter within country A.			

If the interface ih is PSTN-based an interworking unit shall transform the SIP information elements received from the ESRF into PSTN signalling.

The mapping shall support a mechanism for the transfer of the network provided location information. Since ih is an internal interface the mapping between SIP and PSTN is a national matter within country A in the architecture in ETSI ES 203 178 [1]. Table 5.11 describes a guideline using ETSI TS 129 163 [14] for the mapping between mandatory information elements defined in ETSI ES 203 178 [1] and ISUP protocol elements.

In table 5.11 column 1 represents the Information Element (IE) in ETSI ES 203 178 [1]. Column 2 lists the relevant specifications, for which requirements are described in column 4. Column 3 specifies the parameters in ISUP that maps to this IE in ETSI ES 203 178 [1]. Column 4 contains requirements and additional information.

Table 5.11: ih interface PSTN case-based

IE	Specifications	ISUP Parameter	Requirements and additional information
Called Identity	ETSI TS 129 163 [14]	Called party number	The E.164 address encoded in either the Request-URI or the Route header field of the ESRF is mapped to the called party number parameter. If the Request-URI contains a SIP or tel URI then the value in the Request-URI shall be used. If the Request-URI contains a Service URN then the value in the Route header field shall be used (see note).
Network-provided caller identity	ETSI TS 129 163 [14]	Calling party number	The E.164 address encoded in the P-Asserted-Identity header field is mapped to the Calling party number parameter. The setting of the Calling Party number parameter APRI is depending on the SIP Privacy header field.
Network-provided location information	n/a	n/a	The mapping of the network-provided location information from SIP to PSTN or the use of other PSTN information elements, e.g. the network provided caller identity as a location reference, is a national matter within country A.
User-provided caller identity	ETSI TS 129 163 [14]	Generic number (Additional calling party number)	If the From header field contains an E.164 number, the From header field is mapped to the Generic number (Additional Calling Party Number) parameter. The setting of the Generic Number parameter APRI is depending on the SIP Privacy header field.
User-provided location information	n/a	n/a	The mapping of the user-provided location information from SIP to PSTN is a national matter within country A.
Push correlation identifier	n/a	n/a	The mapping of the push correlation identifier from SIP to PSTN is a national matter within country A.
VSP identity	n/a	n/a	The mapping of the VSP identity from SIP to PSTN is a national matter within country A.
NOTE: ETSI TS 129 163 [14] does not define a mapping of a Route header field into a Called party number.			

5.8.2 IMS implementation considerations

In the case where the ECSP and PSP are both IMS but are run by different operators then Inter-IMS Network to Network Interface protocol, as specified in ETSI TS 129 165 [11], applies.

The interface Ici of ETSI TS 129 165 [11] conforms to the interface ih.

In the context of the present document, the non-roaming II-NNI traversal scenario (originating home network - terminating home network) applies to the interface ih.

Location-based information shall be exchanged according to clause 5.8.1 of the present document.

In the case where the ECSP and the PSP are both IMS and are run by the same operator the interface ih becomes an internal interface and ETSI TS 124 229 [10] applies, as specified for the interface at the Mw reference point or at the Ici reference point, if the IP-PSAP is connected in peering-based mode according to the business trunking architecture [33].

If the ECSP has deployed a SIP-based IP network and the PSP is a different operator with IMS or vice versa, the ECSP shall appear to the PSP as if it were an IBCF complying with the requirements identified in ETSI TS 124 229 [10], clause 4.1 for this functional entity. When processing an emergency call, IBCF implementations are expected to be transparent to unrecognized information unless specific exceptions exist.

Location-based information shall be exchanged according clause 5.8.1 of the present document.

5.9 Interface ii

5.9.1 Protocol specifications

The interface ii is located between the ESRP and the PSTN-PSAP. According to ETSI ES 203 178 [1], this is an internal interface inside country A. Table 5.12 is based on table 5.11 and the previous protocol interworking. Table 5.12 describes a guideline for the mapping between information elements defined in ETSI ES 203 178 [1] and DSS1 information elements.

In table 5.12 column 1 represents the Information Element (IE) in ETSI ES 203 178 [1]. Column 2 lists the relevant specifications, for which requirements are described in column 4. Column 3 specifies the DSS1 information element that maps to this IE in ETSI ES 203 178 [1]. Column 4 contains requirements and additional information.

Table 5.12: Interface ii ESRP - PSTN-PSAP

IE	Specifications	DSS1 information element	Requirements and additional information
Called Identity	ETSI EN 300 899-1 [34]	Called party number	E.164 address of the PSAP encoded called party number information element.
Network-provided caller identity	ETSI EN 300 899-1 [34]	Calling party number	Network-provided E.164 address of the emergency caller encoded in the calling party number information element. The availability of the network-provided caller identity depends on the privacy behaviour of the ESRP. The setting of the Calling Party number parameter APRI is depending on the SIP Privacy header field provided by the ESRF and the privacy handling of the ESRP.
Network-provided location information	n/a	n/a	The use of specific PSTN information elements conveying network-provided location information is a national matter within country A.
User-provided caller identity	ETSI EN 300 899-1 [34]	Additional calling party number	User-provided E.164 number of the emergency caller encoded in the additional calling party number information element. The availability of the user-provided caller identity depends on the network implementation and the privacy behaviour of the ESRP. The setting of the additional calling party number parameter APRI is depending on the SIP Privacy header field provided by the ESRF.
User-provided location information	n/a	n/a	The use of specific PSTN information elements conveying user-provided location information is a national matter within country A.
Push correlation identifier	n/a	n/a	The use of specific PSTN information elements conveying a push correlation identifier is a national matter within country A.
VSP identity	n/a	n/a	The use of specific PSTN information elements conveying the VSP identity is a national matter within country A.

5.9.2 IMS implementation considerations

This is the interface between the ESRP and the PSTN-PSAP. It is outside the scope of IMS.

5.10 Interface ij

5.10.1 Protocol specifications

The interface ij is located between the ESRP and the IP-PSAP. According to ETSI ES 203 178 [1], this is an internal interface inside country A. If SIP is used across this interface, table 5.13 describes the mapping between information elements defined in ETSI ES 203 178 [1] to be conveyed across the ij interface and the specifications containing the relevant SIP header fields.

In table 5.13 column 1 represents the Information Element (IE) in ETSI ES 203 178 [1]. Column 2 lists the relevant specifications, for which normative requirements are described in column 4. Column 3 specifies the header fields in SIP that maps to this IE in ETSI ES 203 178 [1]. Column 4 contains requirements and additional information.

Table 5.13: Interface ij ESRP - IP-PSAP

IE	Specifications	SIP header field	Requirements and additional information
Called Identity	IETF RFC 3261 [3] IETF RFC 6881 [27]	Request URI or Route header field (see note)	The PSAP address as received from the ESRP in the context of national requirements applicable to emergency services.
Network-provided caller identity	IETF RFC 3325 [28]	P-Asserted-Identity	If the VSP sends a P-Asserted-Identity, the ESRF and the ESRP shall pass it transparently.
Network-provided location information	IETF RFC 6442 [7] IETF RFC 4119 [15] IETF RFC 5139 [16] IETF RFC 5491 [17] IETF RFC 6848 [18]	Geolocation	The Geolocation header field indicates that the SIP message, in this case an INVITE, contains either a location value or a location URI depending on the value in the header. The SIP Geolocation Header field is defined in IETF RFC 6442 [7]. IETF RFC 4119 [15] defines so called Presence Information Data Format - Location Objects (PIDF-LO) which are used by IETF RFC 6442 [7]. Further PIDF-LO types are defined by IETF RFC 5139 [16]. General information on how to constrain, represent, and interpret locations in a PIDF-LO are described in IETF RFC 5491 [17]. IETF RFC 6848 describes how new civic address elements are added [18]. ETSI ES 203 178 [1] supports multiple location sources adding location to the call. Location ordering as defined in IETF RFC 6442 [7] applies. Location information may be location-by-value in the form of a PIDF-LO contained in the body of the SIP INVITE message, or a location reference in the form of a location URI conforming to the HTTP(S) or SIP(S) URI schemes. In addition to ordering it is necessary to know the identity of the entity adding location information to the call so that downstream entities can decide in which provider of location they have more confidence. This accomplished using the loc-src parameter defined in draft-winterbottom-sipcore-locparam-01 [36].
User-provided caller identity	IETF RFC 3261 [3]	From	The identity of the UE conveyed over ia is mapped to the SIP From header field by the VSP. The value in the From header field is copied from ih to ij.
User-provided location information	IETF RFC 6442 [7] IETF RFC 4119 [15] IETF RFC 5139 [16] IETF RFC 5491 [17] IETF RFC 6848 [18]	Geolocation Geolocation-Routing	The Geolocation header field indicates that the SIP message, in this case an INVITE, contains either a location value or a location URI depending on the value in the header. The SIP Geolocation Header field is defined in IETF RFC 6442 [7]. IETF RFC 4119 [15] defines so called Presence Information Data Format - Location Objects (PIDF-LO) which are used by IETF RFC 6442 [7]. Further PIDF-LO types are defined by IETF RFC 5139 [16]. General information on how to constrain, represent, and interpret locations in a PIDF-LO are described in IETF RFC 5491 [17]. IETF RFC 6848 describes how new civic address elements are added [18]. The Geolocation-Routing header field explicitly grants permission for the location information to be used for routing. The values are comma separated in the same Geolocation header field. Provision has been made for each location value to have a generic-param defined, but does not currently define any parameters.

IE	Specifications	SIP header field	Requirements and additional information
			ETSI ES 203 178 [1] supports multiple location sources adding location to the call. Location ordering as defined in IETF RFC 6442 [7] applies. Location information may be location-by-value in the form of a PIDF-LO contained in the body of the SIP INVITE message, or a location reference in the form of a location URI conforming to the HTTP(S) or SIP(S) URI schemes. In addition to ordering it is necessary to know the identity of the entity adding location information to the call so that downstream entities can decide in which provider of location they have more confidence. This accomplished using the loc-src parameter defined in draft-winterbottom-sipcore-locparam-01 [36].
IP address and port	IETF RFC 3261 [3]	Via	The value in the Via header field is copied from ih to ij, if received via the ih interface. The bottommost Via header field added by the UE contains the IP address and port of the UE.
VSP identity	IETF RFC 7852 [29]	ProviderInfo	The VSP identity is either a MIME component in the body of the SIP INVITE or a data field stored on an external repository. The SIP Call-Info header field of the SIP INVITE contains a URI pointing to the ProviderInfo. In the first case, the URI in the Call-Info-header is a CID URI, in the second case it is a pointer (e.g. a HTTPS URI) which can be dereferenced by authorized third parties (e.g. a PSAP). The ProviderInfo includes the following data elements: DataProviderReference DataProviderString ProviderID ProviderIDSeries TypeOfProvider: Value "Telecom Provider" Language DataProviderContact This element might not be received via the interface ih if national regulation does not require it, or if the identity can be inferred from the Network-provided caller identity. If the VSP identity is passed on, than the ESRP shall pass on the VSP identity as received, without modification.
NOTE: When the Called Identity is mapped to the Route header field, the Request URI shall contain the original Service URN. When the Called Identity is mapped to the Request URI it shall contain a SIP URI or a telURI. The choice between the two mapping options is a national matter within country A.			

5.10.2 IMS/NGN implementation considerations

This is the interface between the ESRP and the IP-PSAP.

IMS covers the case in which IP-PSAP is a user equipment (UE).

In this case the interface ij corresponds to the Gm reference point for IMS-based access domain (as described in ETSI TS 124 229 [10]), with the exception that an emergency call will be an incoming call.

5.11 Interface ik

5.11.1 Protocol specifications

The interface ik is located between the PSTN-PSAP and the ESRF or between the PSTN-PSAP and the LS-Proxy. According to ETSI ES 203 178 [1], this is an internal interface inside country A. Tables 5.14 and 5.15 describe a guideline for the mapping between information elements defined in ETSI ES 203 178 [1] to be conveyed across the ik interface. In the case that interface ik is not currently implemented, a protocol such as the HELD dereference specification [25] may be considered.

In this case, upon receipt of a location URI or a network-based caller identity the PSTN-PSAP shall initiate location dereferencing according to the IETF HELD dereference specification IETF RFC 6753 [25].

In table 5.14 column 1 represents the element name of the HELD protocol. Column 2 indicates the status of this element (mandatory, conditional or optional). Column 3 describes additional requirements and the mapping of the element to the information element (IE) in ETSI ES 203 178 [1]. Column 4 specifies the permitted values for the element in column 1.

Table 5.14: HELD Location Request

HELD Element Name	Status in HELD	Description and related ETSI ES 203 178 [1] Information element with (Status in ETSI ES 203 178)	Value
responseTime	M	The time in which the requesting entity would like a response in ms. Not defined in ETSI ES 203 178.	The responseTime in the HELD locationRequest shall be set to "emergencyDispatch"
locationType	M	Specifies the form that the requesting entity would like the location to come in. Not defined in ETSI ES 203 178.	civic or geodetic
exact	M	Specifies whether the server returns an error if the requested locationType is not available. Not defined in ETSI ES 203 178.	False
locationURI	C	URI to be used to retrieve a location value (see note). ETSI ES 203 178: location reference (O), location identifier (O).	locationURI, expires
device	C	If a locationURI is not available, the PSTN-PSAP shall provide a device identifier according to IETF RFC 6155 [22] (see note). ETSI ES 203 178: Network-provided caller identity (O).	Device identifier according to IETF RFC 6155 [22]
NOTE: Either a locationURI or a device identifier shall be included.			

In table 5.15 column 1 represents the element name of the HELD protocol. Column 2 indicates the status of this element (mandatory, conditional or optional). Column 3 describes additional requirements and the mapping of the element to the information element (IE) in ETSI ES 203 178 [1]. Column 4 specifies the permitted values for the element in column 1.

Table 5.15: HELD Location Response

HELD Element Name	Status in HELD	Description and related ETSI ES 203 178 [1] Information element with (Status in ETSI ES 203 178)	Value
Presence	M	The ESRF or the LS-Proxy shall return a location value, either civic, geodetic or both. ETSI ES 203 178: location value (M).	Location-info (PIDF-LO)

The use of the location push mode via interface ik is a national matter. This may apply, if the encoding of a location value is not supported towards the PSTN-PSAP.

If the network-based caller identity cannot be used, the ESRF shall send a push correlation identifier to the PSTN-PSAP. The determination of the protocol to support the location push mode and the format of the push correlation identifier is a national matter.

5.11.2 IMS/NGN implementation considerations

This is the interface between the PSTN-PSAP and the ESRF/LS-Proxy.

This interface is not part of the IMS architecture as specified in ETSI TS 123 228 [i.4] and it is not part of the NGN architecture as specified in ETSI ES 282 001 [i.1].

This interface corresponds to Le reference point for IMS-based networks described in ETSI TS 123 167 [12].

5.12 Interface il

5.12.1 Protocol specifications

The interface il is located between the IP-PSAP and the LS. According to ETSI ES 203 178 [1], this is an internal interface inside country A. Tables 5.16 and 5.17 describe a guideline for the mapping between information elements defined in ETSI ES 203 178 [1] to be conveyed across the il interface. In the case that interface il is not currently implemented, a protocol such as the HELD dereference specification [25] may be considered.

In this case, upon receipt of a location URI the IP-PSAP shall initiate location dereferencing according to the IETF HELD dereference specification IETF RFC 6753 [25].

In table 5.16 column 1 represents the element name of the HELD protocol. Column 2 indicates the status of this element (mandatory, conditional or optional). Column 3 describes additional requirements and the mapping of the element to the information element (IE) in ETSI ES 203 178 [1]. Column 4 specifies the permitted values for the element in column 1.

Table 5.16: HELD Location Request

HELD Element Name	Status in HELD	Description and related ETSI ES 203 178 [1] Information element with (Status in ETSI ES 203 178 [1])	Value
responseTime	M	The time in which the requesting entity would like a response in ms. Not defined in ETSI ES 203 178 [1].	The responseTime in the HELD locationRequest shall be set to "emergencyDispatch"
locationType	M	Specifies the form that the requesting entity would like the location to come in. Not defined in ETSI ES 203 178 [1].	civic or geodetic
exact	M	Specifies whether the server returns an error if the requested locationType is not available. Not defined in ETSI ES 203 178 [1].	False
locationURI	M	URI to be used to retrieve a location value The location URI shall contain a location reference or a location identifier. ETSI ES 203 178 [1]: location reference (O), location identifier (O).	locationURI, expires

In table 5.17 column 1 represents the element name of the HELD protocol. Column 2 indicates the status of this element (mandatory, conditional or optional). Column 3 describes additional requirements and the mapping of the element to the information element (IE) in ETSI ES 203 178 [1]. Column 4 specifies the permitted values for the element in column 1.

Table 5.17: HELD Location Response

HELD Element Name	Status in HELD	Description and related ETSI ES 203 178 [1] Information element with (Status in ETSI ES 203 178 [1])	Value
Presence	M	The location server shall return a location value, either civic, geodetic or both. ETSI ES 203 178 [1]: location value (M).	Location-info (PIDF-LO)

5.12.2 IMS implementation considerations

This is the interface between the IP-PSAP and the Location Server. This is not an IMS reference point.

It could be a web service-based interface.

5.13 Interface im

5.13.1 Protocol specifications

The interface im is located between the IP-PSAP and the LS-Proxy. According to ETSI ES 203 178 [1], this is an internal interface inside country A. Tables 5.18 and 5.19 describe a guideline for the mapping between information elements defined in ETSI ES 203 178 [1] to be conveyed across the im interface. In the case that interface im is not currently implemented, a protocol such as the HELD dereference specification [25] may be considered.

In this case, upon receipt of a location URI or a network-based caller identity the IP-PSAP shall initiate location dereferencing according to the IETF HELD dereference specification IETF RFC 6753 [25].

In table 5.18 column 1 represents the element name of the HELD protocol. Column 2 indicates the status of this element (mandatory, conditional or optional). Column 3 describes additional requirements and the mapping of the element to the information element (IE) in ETSI ES 203 178 [1]. Column 4 specifies the permitted values for the element in column 1.

Table 5.18: HELD Location Request

HELD Element Name	Status in HELD	Description and related ETSI ES 203 178 [1] Information element with (Status in HELD)	Value
responseTime	M	The time in which the requesting entity would like a response in ms. Not defined in ETSI ES 203 178 [1].	The responseTime in the HELD locationRequest shall be set to "emergencyDispatch"
locationType	M	Specifies the form that the requesting entity would like the location to come in. Not defined in ETSI ES 203 178 [1].	civic or geodetic
exact	M	Specifies whether the server returns an error if the requested locationType is not available. Not defined in ETSI ES 203 178 [1].	False
locationURI	C	URI to be used to retrieve a location value (see note). ETSI ES 203 178 [1]: location reference (O), location identifier (O).	locationURI, expires
device	C	If a locationURI is not available, the IP-PSAP shall provide a device identifier according to IETF RFC 6155 [22] (see note). ETSI ES 203 178 [1]: Network-provided caller identity (O).	Device identifier according to IETF RFC 6155 [22]
NOTE: Either a locationURI or a device identifier shall be included.			

In table 5.19 column 1 represents the element name of the HELD protocol. Column 2 indicates the status of this element (mandatory, conditional or optional). Column 3 describes additional requirements and the mapping of the element to the information element (IE) in ETSI ES 203 178 [1]. Column 4 specifies the permitted values for the element in column 1.

Table 5.19: HELD Location Response

HELD Element Name	Status in HELD	Description and the related ETSI ES 203 178 [1] Information element with (Status in ETSI ES 203 178 [1])	Value
Presence	M	The LS-Proxy shall return a location value, either civic, geodetic or both. ETSI ES 203 178 [1]: location value (M).	Location-info (PIDF-LO)

5.13.2 IMS implementation considerations

This is the interface between the IP-PSAP and the ESRF/LS-Proxy.

This interface corresponds to Le reference point for IMS-based network (as described in ETSI TS 123 167 [12]).

5.14 Interface in

5.14.1 Protocol specifications

The in interface is used between the ESRF and the LS-Proxy within the ECSP domain to support the implementation option where these two functional entities are not co-located.

The ESRF shall provide either a location reference or a location identifier to receive a location value from the LS-Proxy.

Furthermore, for example under the following conditions, the ESRF may send a creation context message to the LS-Proxy:

- no mechanism to deliver a location information to a PSTN-PSAP via interface ii;
- PSTN-PSAP uses pull mode via interface ik for retrieval of the location value;
- PSTN-PSAP does not have a location reference or a location identifier, and therefore uses the network-based caller identity as look-up key when using pull mode;
- VSP delivers network-based caller identity in a form that is not compatible to PSTN (e.g.: sip:bob@example.com).

In this case the ESRF can require a binding of the network-based caller identity and a location reference (created by the LS-Proxy) via interface in.

The LS-Proxy sends a response to the ESRF including a location reference that can be delivered to the PSTN-PSAP. Upon the receipt of the location reference the PSTN-PSAP may require location dereferencing via interface ik. For this procedure the LS-Proxy is using the network-based caller id as look-up key for dereferencing via interface if towards the LS.

On completion of the emergency call, the ESRF requires the deletion of the call context.

If no LS-Proxy is implemented the interface in coincides with interface if.

5.14.2 IMS implementation considerations

This is the interface between the ESRF and the LS-Proxy.

This interface is not part of the architecture for IMS emergency sessions [12].

6 Functional entities

6.1 UE

If a UE has sent an emergency call as an anonymous call or requested privacy, or settings in the VSP have made the call as anonymous, this call might be rejected due to the reason that a receiving entity does not allow the restriction of the identity.

6.2 Location Server

The LS shall send the location information either in the form of Location-by-Value (LbyV) or Location-by-Reference (LbyR). If the protocol specified in ETSI ES 283 035 [13] is supported, the LS may send location information in the form of a location identifier.

If the LS supplies LbyR to the VSP, the LS shall also provide a HTTP-enabled dereferencing function [25] for the location URI.

NOTE: All entities providing a dereference function will assume that HELD is supported as a dereference protocol.

6.3 LS Discovery

No specific requirements are defined for this functional entity in the present document. See requirements in clause 5.2.1 for interface ib.

6.4 VSP Call Control

If the VSP Call Control is not able to retrieve location and routeing information it shall use the lowest entry in the via header field that does not contain a private IP address. From this entry it shall use the FQDN or public IP address to determine the regulatory domain of the UE and, if a default PSAP is defined within this specific regulatory domain, shall route the emergency call to this default PSAP. The determination of a default PSAP is a national matter.

The VSP may receive a privacy request during an emergency call set-up or a privacy request can be a permanent subscription for a specific user.

If the VSP receives a privacy request and a trust relationship exists between the VSP and the VAP or between the VSP and the ECSP, the VSP call control shall provide network-provided caller identity and network-provided location information accompanied by a privacy indication. The VSP call control shall not remove the privacy indication.

If identity of the calling user is required by a receiving entity, an anonymous call request can be rejected containing a 433 (Anonymity Disallowed) response to the INVITE request as defined in IETF RFC 5079 [31].

In this case, the VSP shall:

a) if the VSP is permitted to override the privacy of the original INVITE request, send a new INVITE request with identical contents to the original INVITE request, but this time including the identity of the calling user, if absent, and removing any privacy indication;

NOTE: How the permission is obtained (e.g. prior agreement with the calling user) is out of scope of the present document.

b) if the VSP is not permitted to override the privacy of the original INVITE request, relay the response back to the originator of the emergency call request.

In the case that no trust relationship exists between the VSP and the VAP or between the VSP and the ECSP, the VSP call control is allowed to restrict the network provided caller identity, but has to consider the consequence that the call might get rejected by the ECSP.

6.5 Emergency Service Routing Function (ESRF)

6.5.1 Retrieval of the PSAP URI

Upon receipt of an emergency call request with a Request URI containing a urn:service:sos or a specific service type of an emergency category, or a supported emergency public number, via interface ie, the ESRF shall process the network-provided location information. To do this, the ESRF shall be capable of receiving location as a value or a reference. In the case that the ESRF receives a location reference, the ESRF shall initiate a dereferencing procedure using HELD.

When the location value is available, the ESRF shall ignore a Geolocation-Routing header field value and shall determine the URI used to route the emergency call to the correct PSAP. This PSAP URI can be retrieved from local configuration or from an intermediate entity and will either point to an IP-PSAP or to a PSAP connected to the PSTN. In the latter case the request will pass an interworking function before entering the PSTN.

NOTE: This intermediate entity can also be an external server. The address of the external server can be received in the Geolocation header field as specified in IETF RFC 6442 [7].

The mechanisms for selection of PSAP URI are implementation dependent and can be based on a variety of input information.

The structure and the format of the PSAP URI is a national matter within Country A in the architecture in ETSI ES 203 178 [1].

6.5.2 Additional functionalities of the ESRF

Moreover the output of the ESRF towards the next hop shall contain:

- Network-provided caller identity as received from the VSP or the VAP:
  - When no meaningful P-Asserted-Identity header field is present the ESRF shall insert a P-Asserted-Identity header field set to "sip:unavailable@unknown.invalid", if national regulation within country A does not specify anything different.
  - If identity is required by the ESRF to proceed with the emergency call, and this has been withheld by the sending entity, then the ESRF may respond with a 433 (Anonymity Disallowed) response to the INVITE request, as defined in IETF RFC 5079 [31], instead of proceeding with the call.
- Network-provided location information:
  - If an agreement between the ECSP and the PSAP authority or national regulation requires the pull method, the ESRF shall pass the location reference or a location identifier towards the PSAP.
  - In case of emergency calls without or with invalid location information, the ESRF shall route these calls to a default PSAP, if a default PSAP is defined for this case within this regulatory domain. The determination of a default PSAP is a national matter.
- VSP identity:
  - With regard to the VSP identity the emergency call handling by the ESRF is subject to national regulation. It is recommended not to disconnect an emergency call that has sufficient information to be delivered to the correct PSAP, even in the case when a VSP identity (ProviderID, ProviderIDSeries) is unrecognized, e.g. the VSP identity comes from a foreign country with a non-local ProviderIDSeries.
  - If identity is required by the ESRF to proceed with the emergency call, and this is not present in the INVITE request, then the ESRF may respond with a 403 (Forbidden) response to the INVITE request, instead of proceeding with the call.
  - If the VSP identity is passed on, than the ECSP shall pass on the VSP identity as received, without modification.

NOTE: It is possible for the ECSP to contact organizations which provide the ProviderIDSeries and obtain ProviderID allocation for that ProviderIDSeries.

6.5.3 Privacy considerations

If the user requests privacy and national regulation requires the ECSP to provide privacy to the user, and if the ESRF and the ESRP are not in the same trust domain, the ESRF shall prevent the sending of public user identifiers to the PSAP.

The ESRF shall not remove any privacy indicators from the Privacy header field.

The ESRF shall not restrict network-provided location values due to reasons of privacy. The ESRF shall send the network-provided location value, as received from the VSP call control, the VAE or the LS, to the next entity.

NOTE: In many jurisdictions privacy is explicitly disregarded when making emergency calls. Placing an emergency call may disclose user information, including location values towards the PSAP.

6.6 LS Proxy

No specific requirements are defined for this functional entity in the present document.

6.7 Emergency Service Routing Proxy (ESRP)

A national option may exist to override privacy. If the PSAP has an override category regarding network-provided caller identity, the ESRP shall not remove the P-Asserted-Identity header field irrespective of the value of the Privacy header field in accordance with national applied specifications for PSTN- and IP-PSAPs.

If identity is required by the ESRP to proceed with the emergency call, and this has been withheld by the sending entity, then the ESRP may respond with a 433 (Anonymity Disallowed) response to the INVITE request, as defined in IETF RFC 5079 [31], instead of proceeding with the call.

The ESRF shall not restrict network-provided location values due to reasons of privacy.

The ESRP shall send the network-provided location value to the IP-PSAP as received from the ESRF or from an interworking unit in case of a PSTN-PSAP.

If the VSP identity is passed on, than the ESRP shall pass on the VSP identity as received, without modification.

6.8 Route Server

No specific requirements are defined for this functional entity in the present document.

6.9 IP-PSAP

If identity of the calling user is required by the IP-PSAP to proceed with the emergency call, and this has been withheld by the sending entity, then the IP-PSAP may respond with a 433 (Anonymity Disallowed) response to the INVITE request, as defined in IETF RFC 5079 [31], instead of proceeding with the call.

6.10 PSTN-PSAP

If the identity of the calling user is required by the PSTN-PSAP to proceed with the emergency call, and this has been withheld by the sending entity, then the PSTN-PSAP may reject the emergency call, instead of proceeding with the call.

If the PSAP uses anonymous call rejection, the Recommendation ITU-T Q.850 [32] cause code 24 "call rejected due to feature at the destination" can be used to reject the call.

NOTE: In other cases the cause value to be used for anonymous call rejection is a national matter within Country A in the architecture in ETSI ES 203 178 [1].

7 Protocol registration requirements

7.1 General

This clause covers registration of protocol identifiers that are specific to emergency calls. Other registrations that might otherwise be used in a normal call (e.g. country code) are not covered by this clause.

7.2 ProviderIDseries

This portion of the VSP identity is registered with IANA, and the VSP should use one of the existing ProviderIDseries registered with IANA, unless the VSP knows which country (A) the emergency call is routed to and regulation in country A requires a different registration.

Registration details are contained in IETF RFC 7852 [29].

7.3 ProviderID

This portion of the VSP identity is registered by the VSP with the organization identified by the ProviderIDseries.

The option of the fully qualified domain name may be used.

History

Document history		
V1.1.0	September 2017	Membership Approval Procedure MV 20171126: 2017-09-27 to 2017-11-27
V1.1.1	November 2017	Publication