# ETSI TS 123 167 V7.9.0 (2008-06)

Technical Specification

Universal Mobile Telecommunications System (UMTS); IP Multimedia Subsystem (IMS) emergency sessions (3GPP TS 23.167 version 7.9.0 Release 7)

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

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or
perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF).
In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive
within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status.
Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

Intellectual Property Rights

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 (http://webapp.etsi.org/IPR/home.asp).

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.

Foreword

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 3GPP and ETSI identities can be found under http://webapp.etsi.org/key/queryform.asp.

Contents

Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

    x   the first digit:

        1   presented to TSG for information;

        2   presented to TSG for approval;

        3   or greater indicates TSG approved document under change control.

    y   the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

    z   the third digit is incremented when editorial only changes have been incorporated in the document.

1 Scope

This document defines the stage 2 service description for emergency services in the IP Multimedia Core Network Subsystem (IMS), including the elements necessary to support IP Multimedia (IM) emergency services. ITU-T Recommendation I.130 [4] describes a three-stage method for characterisation of telecommunication services, and ITU-T Recommendation Q.65 [3] defines stage 2 of the method.

This document covers also the Access Network aspects that are crucial for the provisioning of IMS emergency services. Other 3GPP specifications that are related to the IMS emergency services are TS 23.228 [1] on IMS in general, including fixed broadband access aspects, and TS 23.234 [7] describing 3GPP/WLAN Interworking and TS 23.271 [5] that covers location services. TS 25.301 [6] contains an overall description of the UMTS Terrestrial Radio Access Network.

GPRS functions for support of IMS emergency services are not defined in this version of the specification.

The emergency support in different IP-CANs is described in the Informative Annex E.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1]   3GPP TS 23.228: "3rd Generation Partnership Project; Technical Specification Group Services and Systems Aspects; IP Multimedia Subsystem (IMS); Stage 2".

[2]   3GPP TS 23.060: "3rd Generation Partnership Project; Technical Specification Group Services and Systems Aspects; General Packet Radio Service (GPRS); Service description; Stage 2".

[3]   CCITT Recommendation Q.65: "Methodology – Stage 2 of the method for the characterisation of services supported by an ISDN".

[4]   ITU Recommendation I.130: "Method for the characterization of telecommunication services supported by an ISDN and network capabilities of an ISDN".

[5]   3GPP TS 23.271: "3rd Generation Partnership Project; Technical Specification Group Services and Systems Aspects; Functional stage 2 description of LCS".

[6]   3GPP TS 25.301: "3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Radio Interface Protocol Architecture".

[7]   3GPP TS 23.234: "3rd Generation Partnership Project; Technical Specification Group Services and Systems Aspects; 3GPP system to Wireless Local Area Network (WLAN) interworking; System description".

[8]   3GPP TS 22.101: "3rd Generation Partnership Project; Technical Specification Group Services and Systems Aspects; Service aspects; Service principles".

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

[10]   IETF Internet-Draft: "Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) Option for Civic Addresses Configuration Information ", draft-ietf-geopriv-dhcp-civil-06 (May 30, 2005).

[11]   3GPP TR 21.905: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Vocabulary for 3GPP Specifications".

[12]   3GPP TS 23.002: "3rd Generation Partnership Project; Technical Specification Group Services and Systems Aspects; Network architecture".

[13]   3GPP TS 24.008: "3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Mobile radio interface Layer 3 specification; Core network protocols; Stage 3".

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

[15]   OMA AD SUPL: "Secure User Plane Location Architecture", http://www.openmobilealliance.org.

[16]   OMA TS ULP: "User Plane Location Protocol", http://www.openmobilealliance.org.

[17]   NENA I2 architecture: "Interim VoIP Architecture for Enhanced 9-1-1 Services (i2)".

[18]   ETSI ES 282 004: "Protocols for Advanced Networking (TISPAN); NGN Functional Architecture; Network Attachment Sub-System (NASS)".

[19]   3GPP TS 24.229: "IP multimedia call control protocol based on SIP and SDP; stage 3".

[20]   3GPP TS 23.203: "Policy and Charging Control architecture".

[21]   3GPP TS 23.003: "Numbering, addressing and identification".

3   Definitions, symbols and abbreviations

3.1   Definitions

For the purposes of the present document, the terms and definitions given in TR 21.905 [11] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in TR 21.905 [11].

Connectivity Session Location and Repository Function (CLF): As per ETSI ES 282 004 [18], the Connectivity Session Location and Repository Function (CLF) registers the association between the IP address allocated to the UE and related network location information, i.e.: access transport equipment characteristics, line identifier (Logical Access ID), IP Edge identity.

Emergency Call Server (ECS): The functional entity consists of a Location Retrieval Function (LRF) and either a routing proxy or a redirect server, e.g. an ECS contains a VPC and a Routing Proxy or Redirect Server in NENA I2 architecture [17].

Emergency-CSCF: The Emergency-CSCF handles certain aspects of emergency sessions, e.g. routing of emergency requests to the correct emergency centre or PSAP.

Emergency Service Query Key (ESQK): A 10-digit North American Numbering Plan number used to identify a particular emergency call instance. It is used by the LRF as a key to look up for the location information and callback information associated with the emergency call instance and is also used by the PSAP to query location information from the LRF.

Emergency Service Routing Key (ESRK): see TS 23.271 [5].

Emergency Service Routing Number (ESRN): North American Numbering Plan number used for routing of an emergency call to the appropriate gateway for an eventual delivery towards a CS-based PSAP.

Geographical Location Information: Location indicated in geographical terms, for example geographical coordinates or street address (e.g. as supported by IETF RFC 4119 [14]).

IP-Connectivity Access Network (IP-CAN): The collection of network entities and interfaces that provides the underlying IP transport connectivity between the UE and the IMS entities**.** An example of an "IP-Connectivity Access Network" is I-WLAN.

Location Identifier: Information about the current location of the UE in the network. Location is indicated in network terms, for example using the global cell id in cellular networks, line-id in fixed broadband networks, (OMA-Location also uses this term, but OMA so far defines the Location Identifier only for cellular access.)

Location Information: The location information may consist of the Location Identifier, and/or the Geographical location information.

Location Retrieval Function (LRF): This functional entity handles the retrieval of location information for the UE including, where required, interim location information, initial location information and updated location information. The LRF may interact with a separate RDF or contain an integrated RDF in order to obtain routing information. The LRF may interact with a separate GMLC or contain an integrated GMLC in order to obtain location information. The LRF may interact with or contain other types of location server functions in order to obtain location information.

Last Routing Option (LRO): A number, which may be used in the event of network failure towards a specific location based PSAP or a number that can be associated to a national or default PSAP/Emergency centre.

Public Safety Answering Point (PSAP): A physical location, where emergency calls from the public are received.

Routing Determination Function (RDF): The functional entity, which may be integrated in a Location Server (e.g. GMLC) or in an LRF, provides the proper PSAP destination address to the E-CSCF for routing the emergency request. It can interact with a location functional entity (e.g. GMLC) to manage ESQK allocation and management, and deliver location information to the PSAP.

3.2 Abbreviations

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

CLF	Connectivity session Location and repository Function
E-CSCF	Emergency-CSCF
ECS	Emergency Call Server
ESQK	Emergency Service Query Key
ESRK	Emergency Service Routing Key
ESRN	Emergency Service Routing Number
LRF	Location Retrieval Function
LRO	Last Routing Option
PSAP	Public Safety Answering Point
RDF	Routing Determination Function

4 High level Principles

4.1 Architectural Principles

The solution for emergency sessions in the IMS fulfils the emergency principles and requirements of TS 22.101 [8] and the following architectural requirements:

1. Void.

2. Emergency services are independent from the IP-CAN with respect to the detection and routing of emergency sessions. The emergency services shall be possible over at least a cellular access network, a fixed broadband access, I-WLAN access and a nomadic access.

3. Any kind of emergency numbers, and emergency SIP and TEL URIs as specified in TS 22.101 [8], and special indications for emergency sessions within the SIP signalling shall be supported.

4. Emergency sessions should be prioritized over non-emergency sessions by the system.

5. The establishment of IMS emergency sessions shall be possible for users with a barred public user identity.

6. The primary solution shall be that the UE can detect an emergency session (e.g. by evaluating the SIP-URI or the dialled number) by itself and indicates the emergency session to the network. The cases where the UE can't detect an emergency session shall also be supported.

7. The solution shall work in case the UE has sufficient credentials to authenticate with the IMS and is registered to the IMS or is not registered with the IMS. The case where the UE does not have sufficient credentials to authenticate with the IMS shall also be supported where regulations allow.

   In the case that UE is not already IMS registered, it shall perform a registration for the support of emergency services (emergency registration).

   In the case a UE is already IMS registered, the UE may skip the additional emergency registration if the UE is aware that it is in its home network (e.g. including IP-CANs where roaming outside the home network is not supported).

   If the UE does not have sufficient credentials to authenticate with the IMS it shall be possible to perform session establishment without an existing security association between UE and P-CSCF, and the UE shall include an equipment identifier (the specific details of the equipment identifier to use may depend upon the IP-CAN) in the request to establish an emergency session.

8. It shall be possible to reject emergency service requests from an UE, without sufficient credentials to authenticate with the IMS in networks where emergency services from UEs with sufficient credentials to authenticate with the IMS are required.

9. Emergency Service is not a subscription service and therefore will mainly be supported in the roamed-to network. In the case that a UE has sufficient credentials, it shall initiate an emergency registration with the network (requiring the involvement of the home network). The CSCFs providing service for emergency sessions may be different from the CSCFs involved in the other IMS services. In the case that the registration fails, the UE may attempt an anonymous emergency call.

10. If an emergency session establishment request is routed to a P-CSCF located in the home network, the home network should be able to detect that the session is for emergency service (whether indicated as such or not) and respond to the UE indicating that the UE should initiate an emergency session in the visited network (e.g. via the CS domain of the visited network).

11. Emergency centers and PSAPs may be connected to the PSTN, CS domain, PS domain or any other packet network.

12. Emergency centres and PSAPs shall be able to call back the user for an emergency session from a UE that has registered (i.e. containing valid credentials).

13. The IMS core network shall be able to transport information on the location of the subscriber.

14. Void.

15. The network shall be able to retrieve the caller's location;

16. As a regional option, the network shall be capable of assigning a routable location key (i.e. Emergency Services Query Key, a.k.a. ESQK, which has the same properties as the existing ESRK in wireless 911 services) to an IMS emergency session, and releasing the ESQK when the emergency session is terminated.

17. The network shall provide the caller's location information to the PSAP upon query from the PSAP.

18. The network shall provide the possibility to route to a default answering point given the scenario where the local PSAP can not be determined.

19. The network may provide a capability to enable a UE to obtain local emergency numbers.

20 A UE should support a capability to obtain local emergency numbers from the network once such a capability has been defined and agreed.

21. It shall be possible to prevent the sending of the information of the users, such as public user identifiers and the location information to the PSAP when explicitly requested by the user, i.e. request on session by session basis.

22. The Emergency Public User Identifier shall only be used for emergency services and not for other services.

NOTE: TS 24.008 [13] contains a procedure to provide local emergency numbers for UMTS and GPRS access but the procedure is not applicable to I-WLAN and contains a limited number of emergency service categories. Therefore, an improved capability may need to be developed for IMS Emergency calls.

In addition to the architectural requirements, the following architectural principles apply to IMS emergency sessions:

- The IMS network shall be able to discriminate between emergency sessions and other sessions. This shall allow special treatment (e.g. with respect to filtering, higher priority, routing, QoS) of emergency sessions.

- If a visited network can support PS emergency service, the emergency session shall be established in the visited network whether or not UE is registered in IMS in the home network.

- The P-CSCF is the IMS network entity, which is responsible to detect the request for emergency session and forwards the request to E-CSCF in the same network.

- The P-CSCF serving the emergency call is the IMS network entity which may retrieve the location identifier from the IP-CAN.

- The E-CSCF is the IMS network entity, which shall be able to retrieve geographical location information from the LRF in the case that the geographical location information is not available and is required.

- If required, the E-CSCF shall be able to forward the location information to the LRF for validation of geographical location information in the case that the geographical location information is included by the UE over any access network type.

- The E-CSCF is the IMS network entity, which is responsible to route the request to an emergency centre/PSAP or BGCF based on location information and additionally other information such as type of emergency service in the request.

4.2 Naming and Addressing

The UE shall use a special emergency Public User Identifier in the emergency registration request. The implicit registration set of the emergency Public User Identifier shall contain an associated Tel URI. The format is defined in TS 23.003 [21].

4.3 Location information for Emergency Sessions

Location information is needed for 2 main reasons in emergency services. The initial purpose of the location information is to enable the IMS network to determine which PSAP serves the area where the UE is currently located, so that the IMS network can route the emergency session to the correct PSAP. The second purpose is for the PSAP to get more accurate or updated location information for the terminal during or after the emergency session.

4.3.1 General Location Information Principles

The following general principles shall apply regarding the handling of location information:

- If the UE has location information available, the UE shall include the location information in the request to establish an emergency session. The location information may consist of network location information, that is the Location Identifier, and/or the Geographical location information.

- The P-CSCF may query the IP-CAN to obtain location identifier. The E-CSCF, if required, may query the LRF for additional location information. If the E-CSCF does not receive location information in the emergency service request, it may query the LRF for location information.

- The E-CSCF shall be able to query the LRF to validate the location information if provided initially by the UE.

- The E-CSCF routes the emergency request to the PSAP/Emergency Centre that corresponds to the current location of the UE or to a default PSAP/Emergency Centre. The access dependent variations of this approach are described below, for the cases where the UE is using I-WLAN or fixed broadband access for the emergency service.

- The E-CSCF forwards the SIP request containing the UE's location information to the PSAP/Emergency Centre or BGCF/MGCF. The location information can contain explicit location information and/or a reference key to allow the PSAP to retrieve location at a later stage.

4.3.2 Void

4.4 IP-CAN

The following are the expectations on the IP-CAN for IMS emergency services:

- It shall be possible to access the IP-CAN without sufficient security credentials.

- It shall be possible to reject requests from UE without sufficient security credentials to establish bearer resources:

  - In the case that the IP-CAN receives a request to establish bearer resources for emergency services, it shall be possible for the IP-CAN to prioritise emergency services traffic. PCC (Policy and Charging Control) methods may be used to inform the IP-CAN and request appropriate handling of the emergency service. The QoS information for emergency traffic is specified in TS 23.203 [20].

- In the case that the IP-CAN receives a request to establish bearer resources for emergency services, the IP-CAN shall ensure that the IP flows using the requested resources are only for communication with the network entities involved in the support of the emergency services. Applicable service data flow filters for emergency traffic need to be defined by the operator according to the details described in TS 23.203 [20].

- The IP-CAN may support emergency services free of charge. Applicable PCC rules need to be defined by the operator according to the details described in TS 23.203 [20].

- The IP-CAN may provide emergency numbers to the UE in order to ensure that local emergency numbers are known to the UE (see TS 22.101 [8]).

The emergency support in different IP-CAN scenarios is described in the Informative Annex E.

5 Architecture model and reference points

5.1 Reference architecture

This specification introduces an additional CSCF role to those defined in the IMS architecture TS 23.002 [12], called Emergency CSCF (E-CSCF), see figure 5.1.
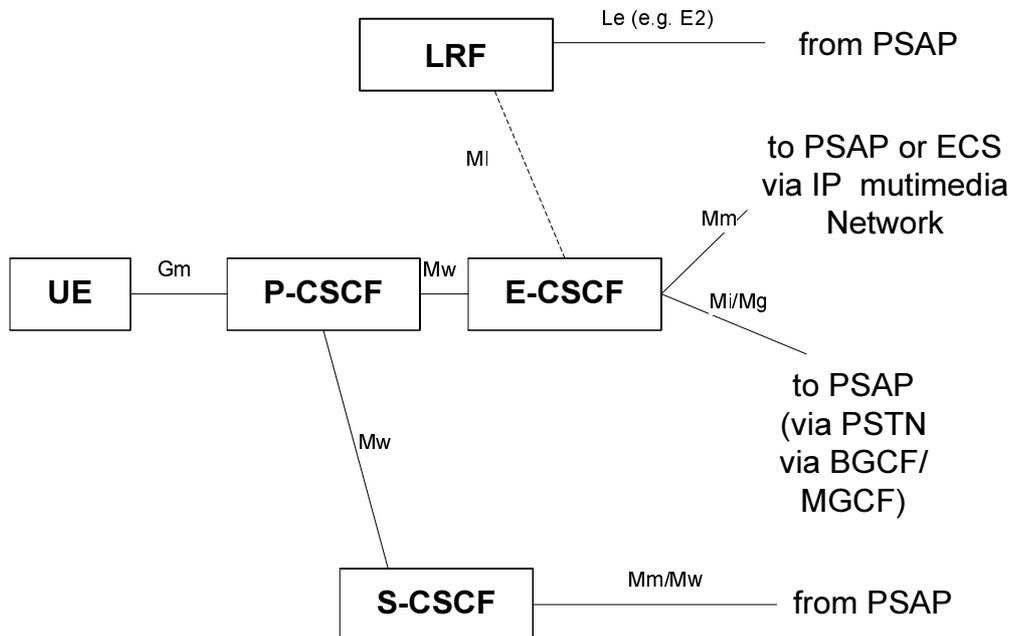
Figure 5.1: E-CSCF in reference architecture

NOTE 1:　P-CSCF and E-CSCF are always located in the same network; this is the visited network when the UE is roaming.

NOTE 2:　For simplicity, not all functional components, e.g. IBCF, I-CSCF, MGCF and BGCF, are shown in this figure.

NOTE 3:　It shall be possible, for example in the North America regions, to support configurations where the Location Retrieval Function (LRF) may consist of a Routing Determination Function (RDF) and a Location Server (e.g. GMLC), the interface between Location Server and RDF is out of scope of this specification. The RDF may be integrated in the Location Server (e.g. in the LRF).

NOTE 4:　Based on local policy, the E-CSCF may route the emergency IMS session to the PSAP via an ECS. See the details in Annex D.

5.2　Reference points

The E-CSCF uses Mw, Mr, Mg, Mi, Ml, and Mm reference points to connect to other IMS entities.

6　Functional description

6.1　UE

- Should be able to detect an emergency session establishment request.

- Use a special emergency Public User Identifier in the IMS emergency registration request.

- The UE may perform an IMS emergency session establishment without prior emergency registration when already IMS registered and it is in home network (e.g. including IP-CANs where roaming outside the home network is not supported).

- Otherwise, the UE shall perform an IMS emergency registration.

- Include an emergency service indication in the emergency session request.

- Include an equipment identifier in the request to establish an emergency session for "anonymous user".

NOTE 1: "Anonymous user" in this context is the person who does not have sufficient credential for IMS registration. No Stage 3 work is expected as the anonymous user detection already existed today.

- Include identity information for the IP-CAN if available (e.g. MCC-MNC or an equivalent)

NOTE 2: UE provided IP-CAN identity information will not be completely reliable and hence a mechanism based on network provision (e.g. using PCC) may be needed in a later version of this specification.

- Attempt the emergency call in CS domain, if capable.

- Handle a 380 (Alternative Service) response with the type set to "emergency" as a result of non UE detectable emergency attempt.

- Handle a response with an indication, IMS emergency registration required as a result of emergency session establishment attempt.

- Other general requirements of UE shall be referred to the general requirements of emergency calls in TS 22.101 [8].

The UE initiates the emergency session establishment request, and for the purpose of processing the request properly in the network the following specific information is supplied in the request message.

- Emergency session indication.

- Emergency Public User Identifier if an IMS emergency registration is performed. If not, any registered Public User Identifier is used.

- Optionally, type of emergency service. It could be implied in the above emergency session indication.

- UE's location information, if available.

- The Tel URI associated to the emergency Public User Identifier, if available.

In the case of a non UE detectable emergency call, upon reception of indication from the P-CSCF, the UE shall handle the call as an emergency session.

NOTE 3: If the indication was received in a rejection message the UE performs appropriate emergency error handling procedures.

6.2   IMS Functional entities

6.2.1   Proxy-CSCF

- Handle registration requests with an emergency Public User Identifier like any other registration request, except that it may reject an emergency registration request if the IM CN subsystem that the P-CSCF belongs to can not support emergency sessions for the UE (e.g., due to local policy or UE is not within IM CN subsystem's geographical area or IP-CAN not supported)..

- Detect an emergency session establishment request.

- Reject/allow unmarked emergency requests.

- Reject/allow anonymous emergency requests.

- Prevent the assertion of an emergency Public User Identifier in non-emergency requests

- Prevent non-emergency requests that are associated with an emergency registration.

- May query IP-CAN for location identifier.

- Select an Emergency CSCF in the same network to handle the emergency session request. The selection method is not standardized in the present document.

- Prioritize the emergency session.

- Check the validity of the caller Tel URI if provided by the UE and shall provide the Tel URI in the session establishment request if it is aware about the Tel URI associated with the emergency Public User Identifier.

- May respond to a UE with an emergency session indication as a result of detecting a non UE detectable emergency session establishment request

- May respond to the UE with an indication, IMS emergency registration required as a result of processing the emergency session establishment attempt.

- Should be able to identify the service data flow associated with emergency service and inform PCRF accordingly.

6.2.2 Emergency-CSCF

- Receive an emergency session establishment request from a P-CSCF.

- If location information is not included in the emergency request or additional location information is required, the E-CSCF may request the LRF to retrieve location information as described in clause 7.6 Retrieving Location information for Emergency Session.

- If required, the E-CSCF requests the LRF to validate the location information if included by the UE.

- Determines or queries the LRF for the proper routing information/PSAP destination.

- Route emergency session establishment requests to an appropriate destination including anonymous session establishment requests.

- Subject to national requirements, the E-CSCF may send the contents of the P-asserted ID or UE identification to the LRF.

- Based on local policy, the E-CSCF may route the emergency IMS call to ECS for further call process.

6.2.3 Location Retrieval Function

The Location Retrieval Function (LRF) is responsible for retrieving the location information of the UE that has initiated an IMS emergency session. It shall be possible to support configurations where the Location Retrieval Function (LRF) may consist of a Routing Determination Function (RDF) and a Location Server (e.g. GMLC), the interface between Location Server and RDF is out of scope of this specification.

The LRF utilizes the RDF to provide the routing information to the E-CSCF for routing the emergency request. The RDF can interact with a location functional entity (e.g., GMLC) and manage ESQK allocation and management. The ESQK is used by the PSAP to query the LRF for location information and optionally a callback number. The LRF-PSAP interactions are outside the scope of this specification.

Information provided by the LRF to the E-CSCF includes the routing information and other parameters necessary for emergency services, which are subject to local regulation. For example, this information may include the ESQK, ESRN, LRO in North America, location number in EU, PSAP SIP URI or Tel URI.

In order to provide the correct PSAP destination address to the E-CSCF, the LRF may require interim location information for the UE.

In some regions, for example in the North American region, it may be a requirement to provide the PSAP with an accurate initial location estimate for the UE and possibly to provide an accurate updated location estimate for the UE if requested by the PSAP. When this requirement exists, the LRF may store a record of the emergency session including all information provided by the E-CSCF and shall only release this record when informed by the E-CSCF that the emergency session has terminated. The information provided by the LRF to the E-CSCF (e.g. ESQK) shall then include correlation information identifying both the LRF and the emergency session record in the LRF. This correlation information shall be transferred to the PSAP during session establishment (e.g. in a SIP INVITE or via SS7 ISUP

signalling from the MGCF). The PSAP may use this information to request an initial location estimate from the LRF and/or to request an updated location estimate.

6.2.4 Serving CSCF

When the S-CSCF receives an Emergency Registration, the S-CSCF determine the duration of the registration by checking the value of the Expires header in the received REGISTER request and based on local policy of the serving system.

> NOTE: The value of the emergency registration time is subject to national regulation and can be subject to roaming agreements.

7 Procedures related to establishment of IMS emergency session

7.1 High Level Procedures for IMS Emergency Services

7.1.1 UE Detectable Emergency Session

The following flow contains a high level description of the emergency service procedures performed when the UE can detect the emergency session is being requested.
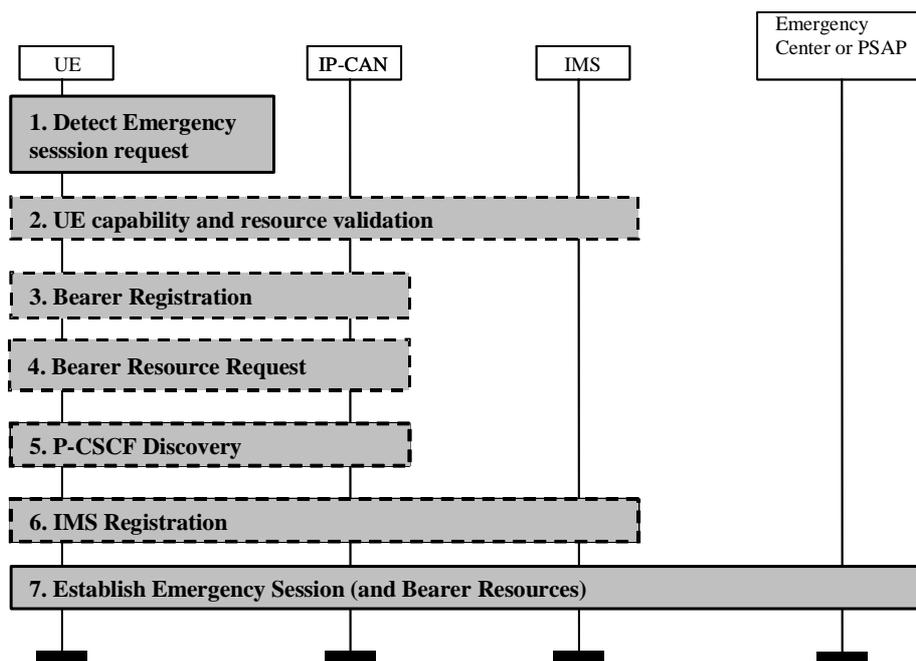
Figure 7.1: Terminal Detected Emergency Calls

The following steps are performed:

1. The UE detects the request for the establishment of an emergency session. Step 2 to 6 may be skipped based on the conditions specified in clause 6.1.

2. In the case that the UE has insufficient resources or capabilities to establish an emergency call due to other ongoing sessions then the UE should terminate the ongoing communication and release reserved bearer resources

3. In the case that bearer registration is required and has not been performed, the UE shall perform bearer registration to the IP-CAN. If the UE is already bearer registered, then the bearer registration procedures are not required to be performed.

   NOTE 1: Depending on the IP-CAN, the UE may be assigned an IP address at this stage.

4. In the case that bearer resources for the transport of the IMS related signalling are required to be reserved in the IP-CAN, the UE shall reserve the resources in the IP-CAN.
   If the IP-CAN does not provide an IP address to the UE in step 3, then the IP-CAN shall allocate an IP address to the UE during the bearer resource request procedures.

5. UE performs a P-CSCF discovery procedure, where the UE discovers a P-CSCF in the local network suitable for use in emergency sessions.

   NOTE 2: The exact means for the P-CSCF discovery is dependant upon the IP-CAN.

6. If the UE has sufficient credentials to authenticate with the IMS network, it shall initiate an IMS emergency registration by providing the IP address obtained at step 3 or step 4 to the P-CSCF selected at step 5. The IP address used for signalling purposes is allocated in association with step 3 or step 4. The IMS registration request shall include an Emergency Public User Identity. The implicit registration set of the emergency Public User Identifier shall contain an associated Tel URI that is used to call back the user from the PSTN.

   The S-CSCF may set the proposed registration expiration according to the local policy of the serving system and regulation. The subsequent registration flows are like any other registration.

   If the UE does not have sufficient credentials to authenticate with the IMS network, it shall not initiate an IMS emergency registration request, but instead immediately establish an emergency session towards the P-CSCF as described in step 7.

7. If IMS emergency registration is performed, the UE shall initiate the IMS emergency session establishment using the IMS session establishment procedures containing an emergency session indication and emergency Public User Identifiers. Otherwise, the UE shall initiate the IMS emergency session establishment using the IMS session establishment procedures containing an emergency session indication and any registered Public User Identifier.

Whether the procedures are activated individually by the UE or some of them are performed automatically depends on the implementation of the terminal and on the UE's configuration. For instance, the multimedia application in the UE could start the application level registration and steps 2-4 would have to be executed in response to support the operation initiated by the application. Interaction with the UE may happen during these steps.

7.1.2 Non UE detectable Emergency Session

As the UE could not detect the emergency session, the session establishment request will be sent to a P-CSCF in the visited PLMN or a P-CSCF in the home PLMN as per a normal session establishment procedure. The former is only applicable to a roaming situation whereas the latter can apply to both a roaming and non-roaming situation. Prior to sending the session establishment request the UE must be registered in the IMS as per the normal registration procedure.

In the case that the P-CSCF detects that this is a request to establish an emergency session, based upon local policy (e.g., checking access type):

- the P-CSCF may reject the session initiation request with an indication that this is for an emergency session. When the UE receives the session rejection then the UE shall either attempt to initiate a call to the dialled number in the CS domain or follow the procedure in 7.1.1.

- If prior attempting the call in the CS domain the UE receives a list of local emergency numbers and recognizes the dialled number as an emergency number, the UE shall attempt an emergency call set up indicating the appropriate emergency call type.

- Alternatively, the P-CSCF in the visited PLMN or the P-CSCF in the home PLMN for a non-roaming UE may allow the session initiation request to continue by inserting the explicit emergency indication in the session request and forward that request to an Emergency CSCF in the same network. The P-CSCF shall inform the UE that the session has been marked as an emergency session so the UE can treat the session as an emergency session establishment.

7.1.3 Emergency Session Establishment using LRF/RDF

Figure 7.2 illustrates a high level call flow for the IMS emergency session establishment procedure using LRF/RDF to retrieve location and routing information.
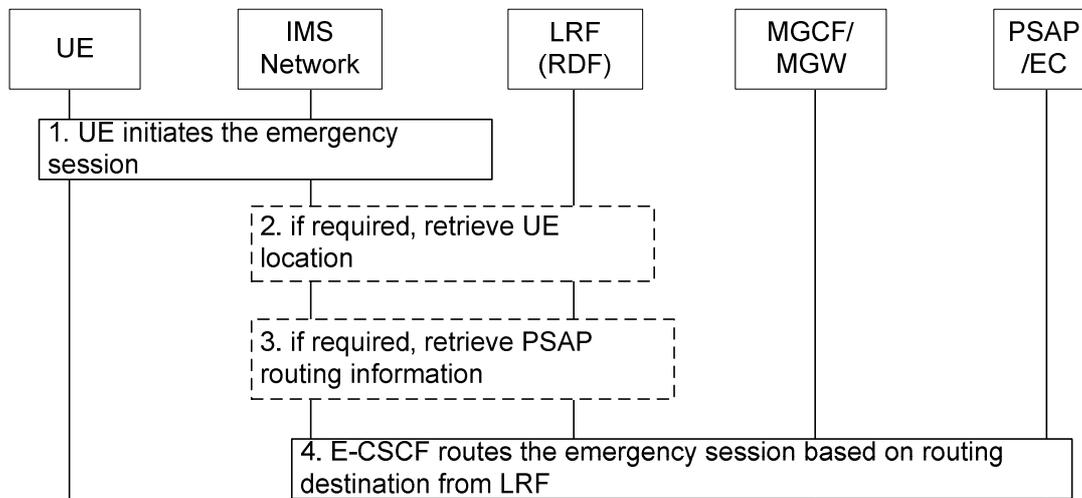

Figure 7.2: Emergency Session Establishment procedure with using LRF/RDF

1. UE initiates an emergency session request by sending a SIP INVITE message with including emergency URI.

2. If required, the IMS network may access the LRF to retrieve the UE's location.

3. If required, LRF invokes the RDF to determine the proper PSAP destination. LRF returns the necessary location/routing information (e.g., ESQK for North America or location number for EU) to the IMS network.

4. The IMS network uses the routing information returned by the LRF to route the emergency session request towards the appropriate PSAP.

NOTE: If the LRF provides an ESQK to the IMS network in step 3 or assigns any other dedicated resource to the emergency session, the IMS network shall inform the LRF when the session is released in order to allow the LRF to release this resource.

7.2 IMS Registration for Emergency Session

The IMS emergency registration procedure shall follow the procedures as described in clause 5.2.2.3 of TS 23.228 [1] with the following modifications:

- The UE shall initiate an IMS emergency registration when all of the following conditions are met:

    - either the UE is not already IMS registered or the UE is IMS registered but is roaming outside its home network;

    - the UE has sufficient credentials to authenticate with the IMS network;

    - the UE is able to detect emergency session.

The UE shall also initiate an IMS emergency registration when it receives an "IMS emergency registration required" response as a result of the emergency session request:

- If the UE initiates an IMS emergency registration, it shall first initiate an emergency access to the IP-CAN if emergency access has been defined for the particular type of IP-CAN. This is to ensure that the session attempt is handled in the VPLMN when the UE is roaming and provides appropriate priority treatment and access to appropriate network elements (e.g. to a particular PDG and P-CSCF in the VPLMN).

- If the UE had already performed an emergency access when it receives an "IMS emergency registration required" response as a result of an emergency registration or emergency session request, it shall perform an emergency access followed by an emergency registration using a different VPLMN if available to prevent looping.

- The UE shall use an emergency Public User Identifier in the emergency registration request. This indication may be used to route calls coming from the PSAP to the contact address registered during the emergency registration procedure and to inform the home network that roaming restrictions may not be applied.

- The user's home network should ignore roaming restrictions for emergency registration requests.

- No originating and terminating services should be applied to emergency Public User Identifiers.

NOTE: The special emergency public user identifier is different from emergency indication in the IMS emergency session establishment request.

P-CSCF handles the registration requests with an emergency Public User Identifier like any other registration request.

The S-CSCF in the home network may modify the received registration expiration value from the request according to local policy in the serving system and regulation. The subsequent registration flows are like any other registration.

7.3   Emergency Session Establishment in the Serving IMS network

If the UE is able to detect that the user is requesting an emergency session then it shall include an emergency service indication in the emergency session establishment request.

If the UE is CS capable and not attached to the PS domain, the UE shall attempt an emergency call in the CS domain. If the UE is only PS attached, and the network has indicated that IMS emergency services are supported, it should attempt the emergency call in the PS Domain. If the UE is attached to both domains, it should follow the requirement as stated in TS 22.101 [8] that specifies "A CS and IMS capable UE attempting an emergency call should give priority to the CS Domain. In case the call attempt fails, the UE should automatically make a second attempt on the other domain". For an attempt in the IM CN Subsystem of the PS domain, the attempt should be in the serving (visited if roaming) IM CN Subsystem of the PS domain.

If the initial attempt is in the CS domain and it fails, the serving (visited if roaming) IM CN Subsystem of the PS domain shall be attempted if the UE is capable. If the initial attempt is in the IM CN Subsystem of the PS domain and it fails, the UE shall make the attempt in the CS domain (if the UE is capable and if for an appropriate service e.g., voice).

If a UE attempts to initiate a session and receives a 380 (Alternative Service) response with the type set to "emergency", the UE shall then re-attempt the session as described above with first attempt being towards the CS domain (if the UE is capable and if for an appropriate service e.g., voice), and with an indication that emergency service is requested.

If the UE is aware that it does not have sufficient credentials to authenticate with the IMS network, it shall not initiate an IMS registration but immediately establish an emergency session towards the P-CSCF, see clause 7.4.

Upon receiving an initial request for an emergency session, the P-CSCF shall follow the rules and procedures described in TS 23.228 [1] with the following additions and clarifications:

- The P-CSCF is the IMS network entity, which detects an emergency session.

- For the case that the initial request carries an indication that the request is for emergency services, and the UE is not registered in the IMS network, see clause 7.4 for details.

- For the case that UE is IMS registered and the initial request does not carry an indication that the request is for emergency services, and the P-CSCF is able to detect that the request is for emergency services, the P-CSCF shall perform the " Non UE detectable Emergency Session " described in clause 7.1.2 above.

- For the case that the initial request carries an indication that the request is for emergency services, and the UE is registered in the IMS network, but not performed emergency registration:

  a) the P-CSCF shall reject the request indicating that IMS emergency registration required, if the UE is roaming;

b) the home P-CSCF may reject the request indicating that IMS emergency registration required, based on local policy.

- On receipt of a session establishment request, which is recognized to be for an emergency service, the P-CSCF shall check whether the UE provided a Tel URI as its identity in the request. If a Tel URI is present in the request, the P-CSCF shall check the validity of this Tel URI. If no Tel URI is present in the request and the P-CSCF is aware about the Tel URI associated with the emergency Public User Identifier, it shall provide the Tel URI to the E-CSCF in the session establishment request.

- The P-CSCF may query the IP-CAN for the location identifier.

- P-CSCF shall prioritize emergency sessions over other non-emergency sessions.

- Emergency IP flows need to be identified by P-CSCF in the Rx interface signalling to allow the PCRF to prioritize emergency service data flows over non-emergency service data flows within IP-CAN. The detailed procedures are specified in TS 23.203 [20].

Upon receiving an initial request for an emergency session from P-CSCF, the E-CSCF shall perform the following:

- if location information is not included in the emergency service request or if additional location information is required, the E-CSCF, if required, retrieves the UE's location information as described in clause 7.6 Retrieving Location information for Emergency Session.

- If location information is included by the UE, the E-CSCF, if required requests the LRF to validate the location information.

- May determine or may request the LRF to determine the appropriate routing information which could be based on the type of emergency service requested and UE's location.

- determine the default PSAP destination if routing based on UE's location is required but the location is unknown.

- If the PSAP/emergency centre contains a point of presence within the IMS connectivity network, the E-CSCF shall forward the emergency session initiation request directly to the PSAP/emergency centre.

- If the PSAP/emergency centre has its point of presence in the PSTN/ISDN network or the CS domain, the E-CSCF uses the Tel-URI obtained from the LRF and forwards the request to an appropriate BGCF/MGCF for routing in the GSTN. This number shall have the same format as used for CS emergency calls. The MGCF may insert any available location information in the PSTN/CS signalling.

NOTE: In case an ESRN is received from the LRF, the E-CSCF maps the received ESRN from the LRF to a TEL-URI before forwarding the request to MGCF.

7.4   IMS Emergency Session Establishment without Registration

When the UE initiates an emergency session establishment without prior IMS registration, it shall include both the "anonymous user" and "emergency service" indications in the emergency session establishment request to the P-CSCF.

Based on local policy, the P-CSCF may reject "anonymous user" emergency session establishment with appropriate error code. UE shall not reattempt the "anonymous user" emergency session again via the same network.

When P-CSCF accepts the "anonymous user" emergency session establishment, it forwards this request to an appropriate E-CSCF although no security association between UE and P-CSCF is established.

The E-CSCF shall follow the same rules and procedure as defined for the Emergency Session Establishment in the Serving IMS network in clause 7.3 to route the anonymous emergency session.

7.5   Interworking with PSAP

7.5.1   PSAP/Emergency centre located at the GSTN

No special procedure is defined. PSAP uses the MSISDN (E.164) of the user for call back.

7.5.2   PSAP/Emergency centre connected via IP using SIP

No special procedure is defined. PSAP uses any public user identity that it has received from the user for call back.

7.5.3   PSAP/Emergency centre connected via ECS

No special procedures are identified in IMS Core, the routing determination will be performed by the ECS.

7.6   Retrieving Location information for Emergency Session

7.6.1   Acquiring location information from the UE or the network

When performing an emergency service, four scenarios for retrieving location information for routing purposes are considered:

- the UE knows its own location;

- the UE retrieves its location information from the network;

- the IMS core retrieves the location information. The related high level procedures are described below;

- location information is not needed to route the emergency call by the IMS core, optionally the emergency routing determination and location information retrieval may be performed by the Emergency Call Server (ECS) as part of the emergency session establishment procedure. In this case, the IMS core does not need to obtain the location information. See the details in Annex D.
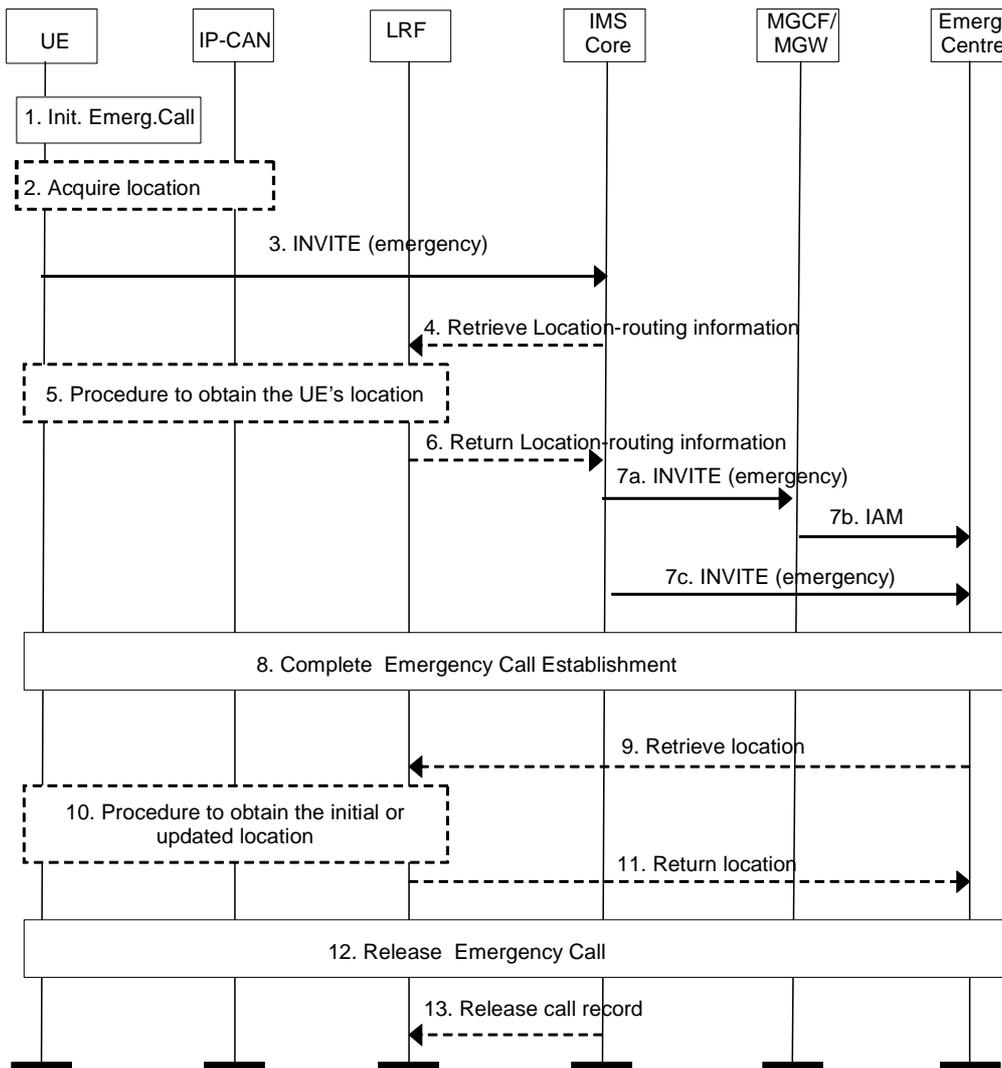
Figure 7.6-1: Handling of location information in IMS emergency calls

1. The user initiates an emergency call.

2. The UE determines its own location or location identifier if possible. If the UE is not able to determine its own location, the UE may, if capable, request its location information from the IP-CAN, if that is supported for the used IP-CAN. If applicable, the IP-CAN delivers to the UE the UE's geographical location information and/or the location identifier.

3. The UE sends an INVITE with an emergency indication to the IMS core. The INVITE should contain any location information that the terminal has. The location information may be geographical location information or a location identifier, which is dependant upon the access network technology. In case the UE is not able to provide any location information, the IMS core may seek to determine the UE's location from the LRF as described below. The INVITE may optionally contain information concerning the location solutions and position methods supported by the UE.

NOTE: the location solutions and position methods conveyed in the INVITE and the means of inclusion in the INVITE are outside the scope of this specification.

4. If the location information provided in step 3 is trusted and sufficient to determine the correct PSAP, the procedure continues from step 7 onwards. If the location information is insufficient or if the IMS core requires emergency routing information, or if the IMS core is required to validate the location information, or if the IMS core is required to map the location identifier received from the UE into the corresponding geographical location information, the IMS core sends a location request to the LRF. The request shall include information identifying the IP-CAN and the UE and may include means to access the UE (e.g. UE's IP address). The request shall also include any location information provided by the UE in step 2. The request may optionally include any information concerning the location solutions and position methods supported by the UE.

5. The LRF may already have the information requested by IMS core or LRF may request the UE's location information. The means to obtain the location information may differ depending on the access technology the UE is using to access the IMS. The SUPL procedures defined in OMA AD SUPL: "Secure User Plane Location Architecture" [15], OMA TS ULP: "User Plane Location Protocol" [16], may be used if supported by the terminal and if it is possible to establish a user plane connection between the UE and the SUPL server. Information provided in step 4 concerning the location solutions and position methods supported by the UE may optionally be used by the LRF to help determine the means to obtain the location information.

   The LRF may invoke an RDF to convert the location information received in step 4 or obtained in step 5 into PSAP routing information, but LRF's interactions with RDF are out of scope of the present specification. The LRF may store the location information, but only for a defined limited time in certain regions, according to regional requirements.

6. The LRF sends the location information and/or the routing information to the IMS core. The LRF may also return correlation information (e.g. ESQK) identifying itself and any record stored in step 5.

7. The IMS core uses the routing information provided in step 6 or selects an emergency centre or PSAP based on location information provided in step 3 or 6 and sends the request including the location information and any correlation information and possibly location information source, e.g., positioning method that was used to obtain the location information to the emergency centre or PSAP.
   7a. The INVITE is sent to an MGCF/MGW,
   7b. The IAM is continued towards the emergency centre or PSAP, or
   7c. The INVITE is sent directly to the emergency centre or PSAP.

8. The emergency call establishment is completed.

9. The PSAP may send a location request to the LRF to get the initial location information for the target UE, or to request LRF to get updated, i.e. current, location information for the target UE. The PSAP may determine the LRF based on the location and/or correlation information received in step 7. The PSAP may also include the correlation information in the request to the LRF.

10. The LRF determines the target UE's location using one of the means listed in step 5 above. The LRF may use the correlation information received in step 9 to retrieve information about the UE that was stored in step 5.

11. The LRF returns the initial or updated location information to the emergency centre or PSAP. As an option for initial location, the LRF may instigate the location step 10 before the request in step 9 is received and may send the initial location to the emergency centre or PSAP either after the request in step 9 is received or before it is received.

12. The emergency call is released.

13. The IMS core may indicate to the LRF that the call is released. The LRF deletes any record stored in step 5.

7.6.2 Void

7.6.3 Void

Annex A (informative):
Void

Annex B (informative): IMS emergency sessions over 3GPP/WLAN Interworking (I-WLAN)

B.1 Void

B.2 Void

B.3 Location handling for I-WLAN

If the UE has location information available, the UE should include the location information in the SIP INVITE request to establish an emergency session. The UE using WLAN access may use the identifier of the access node (e.g. the MAC address of the WLAN Access Point) as the Location Identifier. WLAN UE Originated Procedure in I-WLAN procedure defined in TS 23.271 [5] is applicable to obtain location information.

For regions (e.g. North America) in which an interim location may be required to assist routing to the correct PSAP and/or where accurate initial and updated location information may be required, the IW-MT-LR without HLR/HSS or AAA Query procedure defined in TS 23.271 [5] is applicable.

Annex C (normative): IMS emergency services using Fixed Broadband Access

C.1 Location Retrieval for emergency services over fixed broadband access

These procedures described in this annex apply when the IP-CAN contains a Network Attachment Subsystem with a CLF as specified in ETSI ES 282 004 [18].

C.1.1 High Level Principles for Emergency location information for fixed broadband access

In addition to the architecture described in clause 5.1 above, the P-CSCF has an interface to an LRF which may contain a CLF as described below in figure C.1. For more information on the CLF refer to ETSI ES 282 004 [18].
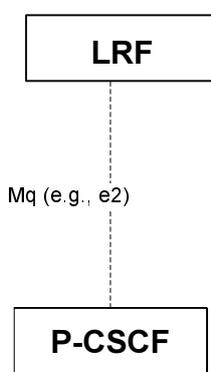
Figure C.1: Additional P-CSCF interface for fixed broadband access

For fixed broadband access, the UE may know its own network location or geographical location. If the UE knows its location, it shall insert the location information in the SIP INVITE request when establishing the emergency IMS session.

As an alternative, if the UE is not able to determine its own location, the UE should try to request its location from the access network. The access network may know the location of the access point where the UE is connected to. The UE should request the location information from the access network according to clause 7.6. The UE shall insert the location information received as a response to the location query in the emergency SIP INVITE request. This location information may be network based, e.g. line identification, or geographical location information.

If the UE does not know its location and is unable to obtain its location from the access network, the UE should have a means to indicate in the emergency SIP INVITE that its location is unknown.

If the UE does not provide location information, the P-CSCF may request location information from the LRF as described in clause 7.6 and insert the location information in the received INVITE request. The IMS network may also request location information from the LRF in the case that verification of the location information provided by the UE is required. After such verification, the IMS network may insert the location information received from the LRF or override the location information received from the UE before routing the request to the PSAP.

C.1.2 Retrieval of location information for emergency services over fixed broadband access

In addition to clause 7.6, the following applies for a fixed broadband access:

- When the UE is requesting to retrieve the location information from IP-CAN, the UE may use the DHCP option for coordinate-based geographic location of the client as specified by IETF in RFC 3825 [9] and the DHCP

option that allows hosts to learn their civic location via DHCP, as specified in the draft-ietf-geopriv-dhcp-civil-06 [10]. This DHCP option shall not be used by an UE on an IP-CAN using 3GPP RAT.

- The line identifier used by the UE with fixed broadband access may be authenticated by the IMS core.

Annex D (informative):
Examples of call flows according to NENA I2 recommendations

This clause provides the examples of call flows according to NENA I2 recommendations [17].

## D.1 ECS redirecting IMS emergency call
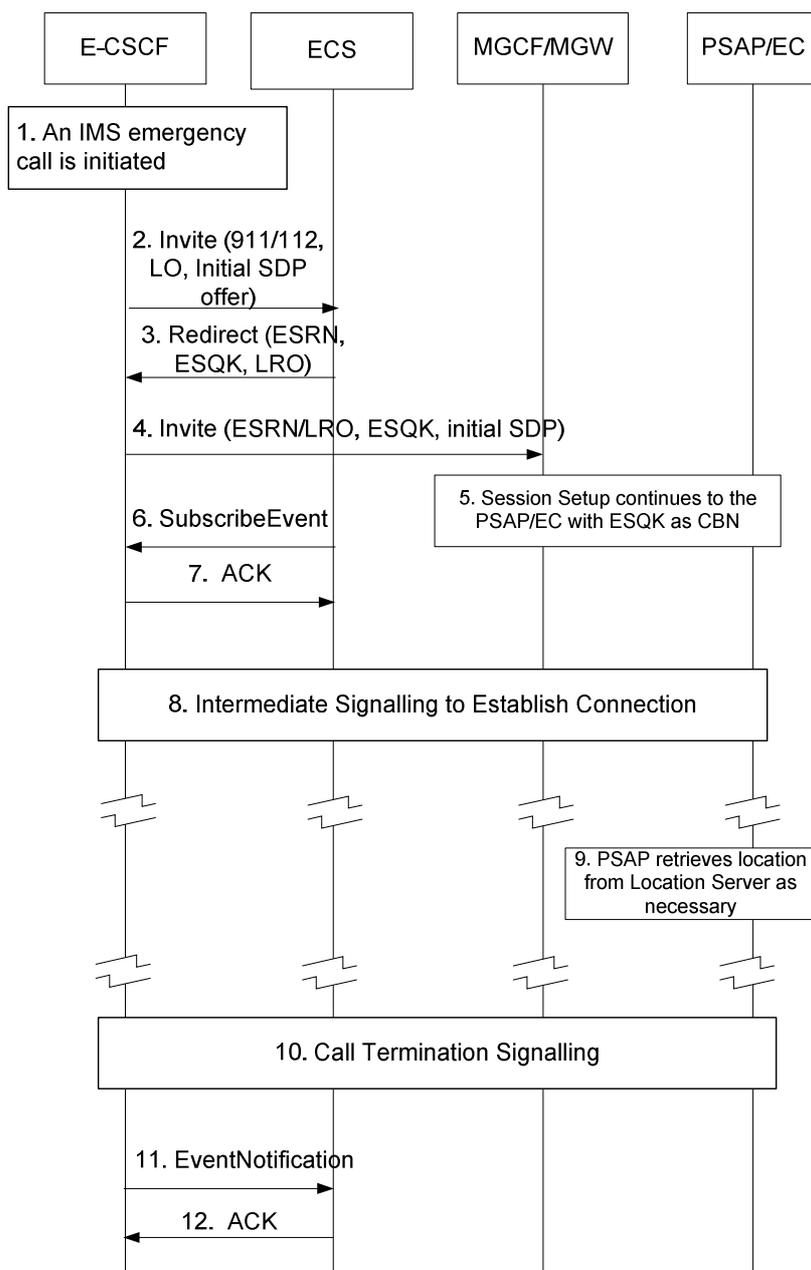
Figure D.1

This flow is supported by the procedures in clause 7.3, where the E-CSCF need not enquire the LRF for location information. Additional steps defined here are standard SIP methods, but not defined in this specification.

Detailed description of the procedure:

1) An IMS emergency call is initiated.

2) The E-CSCF sends an Invite message with 911 or other well known emergency number as the dialled number, the UE's location information in a Location Object (LO) if available, and the UE's media capabilities encapsulated in a SDP payload, to the ECS.

3) Based on the received Location Object (LO), the ECS will determine to which PSAP/EC the call should be routed and allocate an ESQK from the ESQK pool associated with that particular PSAP/EC. The ECS then will format a SIP response with the retrieved ESRN/ESQK in the Contact fields to redirect the emergency call.

4) The IMS Core uses the ESRN/ESQK received in the call redirect message to format an INVITE message properly, and sends it to the MGCF/MGW. A P-Asserted-Identity field may be inserted in the INVITE message, it contains either an ESQK or the CBN.

5) The emergency call setup continues with the PSAP/EC.

6) The ECS initiates a subscription at the IMS Core to request a notification of call termination of the emergency call.

7) An acknowledgement is returned.

8) The emergency session establishment signalling continues.

9) The PSAP retrieves location from the ECS.

10) The emergency session is released.

11) The IMS Core sends an EventNotification message to the ECS with an Event indicating that the 911 call has been terminated. At this time, the ESQK allocated to the emergency session can be released.

12) An acknowledgement is returned to the IMS Core.

D.2 ECS routes the emergency call to the gateway with record route
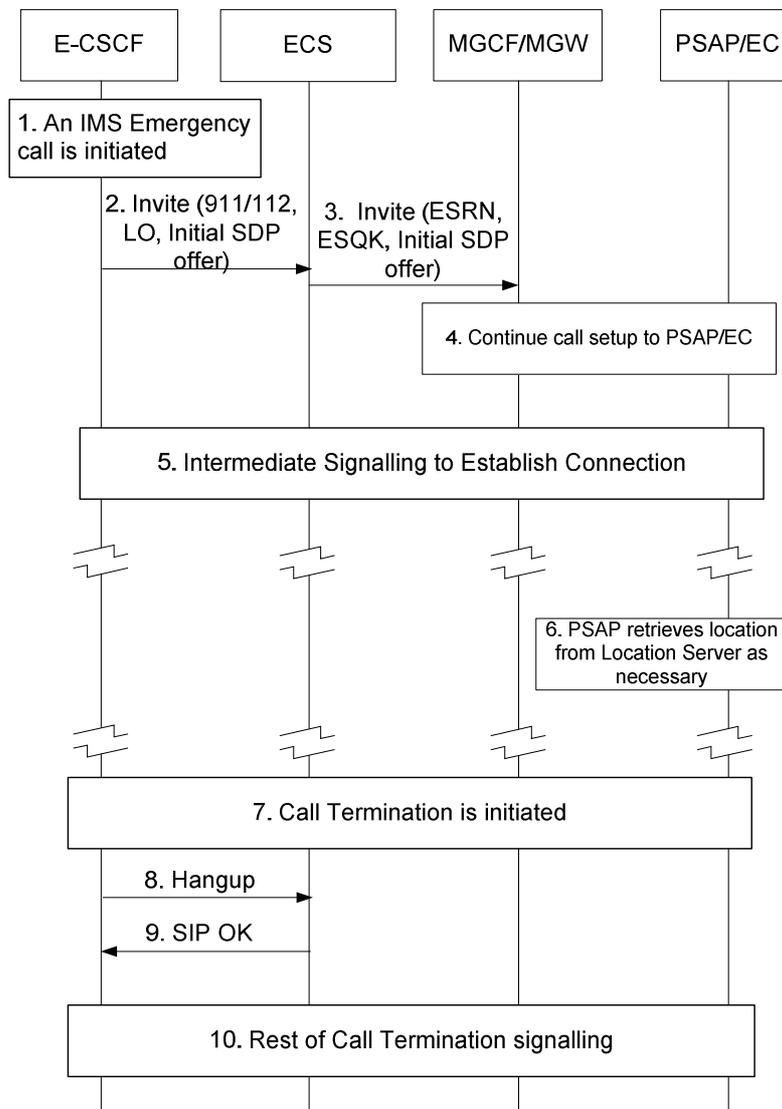
Figure D.2

This flow is supported by the procedures in clause 7.3, where the E-CSCF need not enquire the LRF for location information.

Detailed description of the procedure:

1) An IMS emergency call is initiated.

2) The E-CSCF sends an Invite message with 911 or other well known emergency number as the dialled number, the UE's location information in a Location Object (LO) if available, and the UE's media capabilities encapsulated in a SDP payload, to the ECS.

3) Based on the received Location Object (LO), the ECS will determine to which PSAP/EC the call should be routed and allocate an ESQK from the ESQK pool associated with that particular PSAP/EC. The ECS then re-issues an Invite to an appropriate MGCF/MGW with the ESRN/LRO, ESQK and a record route indication. or the call to be routed to PSAP the P-Asserted-Identity contains ESQK, A P-Asserted-Identity field may be inserted in the INVITE message, f for the call to be routed to other emergency answering centre the P-Asserted-Identity contains the CBN.

4) The emergency call setup continues with the PSAP/EC.

5) The emergency session establishment signalling continues.

6) The PSAP retrieves location from the ECS.

7) Either the caller or PSAP initiates the call termination signalling.

8) The E-CSCF or MGCF/MGW forwards the hangup message to the ECS. At this time, the ESQK allocated to the emergency session can be released.

9) The ECS sends an OK to the E-CSCF or MGCF/MGW.

10) The call termination signalling continues.

Annex E (Informative): Emergency support in different IP-CANs

Support for emergency services in the IP Multimedia Core Network can be provided by certain IP-CANs according to table E.1, which shows the level of possible emergency support in this version of the specification. The UE may be able to use also other IP-CANs that are not included in table E.1 to access emergency services in the IP Multimedia Core Network, but the support of such access technologies is out of scope of this specification.

Table E.1: Support for IMS Emergency Services by Different IP-CANs

IP-CAN	Normal Access	Emergency support	Insufficient Security Credentials
GPRS (note 1)	X		
I-WLAN	X	X	X
Fixed Broadband	X	X	X

NOTE 1: As a PLMN operator option and not as a defined capability in this version of the specification, IMS emergency services using GPRS access could be supported only for an UE that has successfully completed the GPRS Attach/Routeing Area Update procedures with a valid UICC and sufficient security credentials. Specific emergency service procedures for subscribers using a GPRS IP-CAN are not standardised in this release.

The term "normal access" in table E.1 means that the IP-CAN is not made aware of the UE intent to establish an emergency services session and therefore provides no special emergency support e.g. call priority.

The term "emergency support" in the table means that the IP-CAN is made aware of the UE intent to establish an emergency services session, or at least of the priority nature of the access, so that the access network is able to handle the emergency call with appropriate priority.

The term "insufficient security credentials" in the table means that the IP CAN is able to allow a UE with no UICC card or a UICC card with insufficient credentials to obtain IP bearer access for emergency services in the IP Multimedia Core Network.

Annex F (informative): Change history

Change history								
Date	TSG #	TSG Doc.	CR	Rev	Cat	Subject/Comment	Old	New
2006-06	SA#32	SP-060283	0001	3		Basic Call Flows of North America IMS Emergency Session Establishment	7.0.0	7.1.0
2006-06	SA#32	SP-060395	0004	4		Corrections in emergency registration and session request	7.0.0	7.1.0
2006-06	SA#32	SP-060283	0008	1		23.167 Cleanup	7.0.0	7.1.0
2006-06	SA#32	SP-060283	0009	2		Additional Emergency text clarification with regards to NA regional requirements	7.0.0	7.1.0
2006-06	SA#32	SP-060394	0010	3		Location retrieval interface clarification	7.0.0	7.1.0
2006-06	SA#32	SP-060283	0011	2		Addition of missing definitions and abbreviations	7.0.0	7.1.0
2006-06	SA#32	SP-060283	0012	-		Removal of editor's notes on emergency Public User Identifier	7.0.0	7.1.0
2006-06	SA#32	SP-060282	0018	3		Requirement of emergency session establishment without emergency registration	7.0.0	7.1.0
2006-06	SA#32	SP-060283	0021	1		Correction of reference in clause A-4	7.0.0	7.1.0
2006-09	SA#33	SP-060578	0005	2	F	Support of Local Emergency Numbers for IMS Emergency Calls	7.1.0	7.2.0
2006-09	SA#33	SP-060578	0024	1	F	Miscellaneous corrections for IMS Emergency Calls	7.1.0	7.2.0
2006-09	SA#33	SP-060578	0030	3	F	Answers to the GPRS questions in Annex A	7.1.0	7.2.0
2006-12	SA#34	SP-060824	0025	4	C	Blocking of caller's information for emergency communications	7.2.0	7.3.0
2006-12	SA#34	SP-060823	0032	2	F	Clarification to emergency service requirement	7.2.0	7.3.0
2006-12	SA#34	SP-060823	0034	2	F	Change of Annex C title following LS from TISPAN WG2 and approved by SA WG2	7.2.0	7.3.0
2006-12	SA#34	SP-060824	0036	4	C	Addition of source of location information	7.2.0	7.3.0
2006-12	SA#34	SP-060823	0043	1	F	Emergency IMS registration	7.2.0	7.3.0
2006-12	SA#34	SP-060824	0044	2	C	Emergency location information for I-WLAN	7.2.0	7.3.0
2006-12	SA#34	SP-060824	0045	2	B	Restriction to Emergency IMPU	7.2.0	7.3.0
2006-12	SA#34	SP-060823	0049	-	F	Conveying UE Location Capabilities and Clarifying Location Procedures for IMS Emergency Calls	7.2.0	7.3.0
2007-03	SA#35	SP-070086	0038	3	F	GGSN filtering rules	7.3.0	7.4.0
2007-03	SA#35	SP-070086	0050	1	F	Correction to the criteria of IMS emergency registration	7.3.0	7.4.0
2007-03	SA#35	SP-070086	0051	1	F	Correction to XML element and value of 380 response for emergency call with non-emergency registration	7.3.0	7.4.0
2007-03	SA#35	SP-070086	0053	2	F	Rejection of non emergency request with EIMPU	7.3.0	7.4.0
2007-03	SA#35	SP-070086	0054	-	F	Annex B (I-WLAN) cleanup	7.3.0	7.4.0
2007-03	SA#35	SP-070086	0059	1	B	PCC in emergency sessions	7.3.0	7.4.0
2007-03	SA#35	SP-070086	0060	1	F	Correction to Location Information Principle of P-CSCF	7.3.0	7.4.0
2007-03	SA#35	SP-070086	0061	1	C	Setting Emergency Registration Expiration by the Visited Network	7.3.0	7.4.0
2007-03	SA#35	SP-070086	0062	-	F	Functional requirements for GPRS emergency access	7.3.0	7.4.0
2007-03	SA#35	SP-070086	0063	1	B	Use of PCC rules to enforce emergency bearer's usage	7.3.0	7.4.0
2007-06	SA#36	SP-070385	0065	1	F	Align Stage 2 with stage 1 on domain selection for emergency call	7.4.0	7.5.0
2007-06	SA#36	SP-070385	0066	-	F	Editor's note clean up - anonymous rejection by access network	7.4.0	7.5.0
2007-09	SA#37	SP-070535	0067	6	F	IMS Emergency Session Redirection from the Home Network	7.5.0	7.6.0
2007-09	SA#37	SP-070535	0069	3	F	IP-CAN support for IMS Emergency Sessions	7.5.0	7.6.0
2007-12	SA#38	SP-070887	0071	1	F	Correction of Emergency Registration Required 380 Response	7.6.0	7.7.0
2007-12	SA#38	SP-070887	0072	1	F	Cleanup of outstanding issues for IMS Emergency	7.6.0	7.7.0
2007-12	SA#38	SP-070887	0075	1	F	380 response generation	7.6.0	7.7.0
2007-12	SA#38	SP-070887	0077	4	F	P-CSCF procedure clarifications and Emergency Registration time	7.6.0	7.7.0
2008-03	SA#39	SP-080105	0080	1	F	Provide reference to Emergency Public User Identity definition	7.7.0	7.8.0
2008-03	SA#39	SP-080105	0081	1	F	Add P-CSCF procedure to align with 24.229	7.7.0	7.8.0
2008-06	SA#40	SP-080364	0086	1	F	Correction of explanation of roaming	7.8.0	7.9.0
2008-06	SA#40	SP-080364	0089	3	F	Correction to handling of undetectable emergency session	7.8.0	7.9.0
2008-06	SA#40	SP-080364	0091	3	F	UE notification of IMS Emergency Call	7.8.0	7.9.0

History

Document history		
V7.4.0	March 2007	Publication
V7.5.0	June 2007	Publication
V7.6.0	October 2007	Publication
V7.7.0	January 2008	Publication
V7.8.0	April 2008	Publication
V7.9.0	June 2008	Publication