

ETSI TS 123 167 V10.6.0 (2012-07)



Technical Specification

**Universal Mobile Telecommunications System (UMTS);
LTE;
IP Multimedia Subsystem (IMS) emergency sessions
(3GPP TS 23.167 version 10.6.0 Release 10)**



Reference

RTS/TSGS-0223167va60

Keywords

LTE,UMTS

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/chaicor/ETSI_support.asp

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2012.
All rights reserved.

DECT™, PLUGTESTS™, UMTS™ and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.
3GPP™ and LTE™ are Trade Marks of ETSI registered for the benefit of its Members and
of the 3GPP Organizational Partners.
GSM® and the GSM logo are Trade Marks registered and owned by the GSM Association.

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://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.

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

Intellectual Property Rights	2
Foreword.....	2
Foreword.....	5
1 Scope	6
2 References	6
3 Definitions, symbols and abbreviations	8
3.1 Definitions	8
3.2 Abbreviations	9
4 High level Principles	10
4.1 Architectural Principles	10
4.2 Naming and Addressing	12
4.3 Location information for Emergency Sessions.....	12
4.3.1 General Location Information Principles.....	12
4.3.2 Void	13
4.4 IP-CAN	13
5 Architecture model and reference points.....	13
5.1 Reference architecture	13
5.2 Reference points	14
6 Functional description	14
6.1 UE	14
6.2 IMS Functional entities	15
6.2.1 Proxy-CSCF.....	15
6.2.2 Emergency-CSCF	16
6.2.3 Location Retrieval Function	17
6.2.4 Serving-CSCF.....	17
6.2.5 Void	17
6.2.6 Emergency Access Transfer Function (EATF).....	18
6.2.7 Interrogating-CSCF	18
6.2.8 AS	18
6.2.9 HSS	18
7 Procedures related to establishment of IMS emergency session.....	19
7.1 High Level Procedures for IMS Emergency Services	19
7.1.1 UE Detectable Emergency Session.....	19
7.1.2 Non UE detectable Emergency Session.....	20
7.1.3 Emergency Session Establishment using LRF/RDF.....	21
7.2 IMS Registration for Emergency Session	21
7.3 Emergency Session Establishment in the Serving IMS network.....	22
7.4 IMS Emergency Session Establishment without Registration	23
7.5 Interworking with PSAP	24
7.5.1 PSAP/Emergency centre located at the GSTN	24
7.5.2 PSAP/Emergency centre connected via IP using SIP	24
7.5.3 PSAP/Emergency centre connected via ECS.....	24
7.6 Retrieving Location information for Emergency Session	24
7.6.1 Acquiring location information from the UE or the network.....	24
7.6.2 Void	26
7.6.3 Void	26
Annex A (informative): Void	27
Annex B (informative): IMS emergency sessions over 3GPP/WLAN Interworking (I-WLAN)	28
B.1 Void.....	28

B.2	Void.....	28
B.3	Location handling for I-WLAN	28
Annex C (normative):	IMS emergency services using Fixed Broadband Access.....	29
C.1	Location Retrieval for emergency services over fixed broadband access	29
C.1.1	High Level Principles for Emergency location information for fixed broadband access	29
C.1.2	Retrieval of location information for emergency services over fixed broadband access	29
Annex D (informative):	Examples of call flows according to NENA I2 recommendations	31
D.1	ECS redirecting IMS emergency call.....	31
D.2	ECS routes the emergency call to the gateway with record route	33
Annex E (Informative):	Emergency support in different IP-CANs	35
Annex F (normative):	IMS Emergency Services Using HRPD/PDS Network	36
F.1	cdma2000 HRPD/PDS Options.....	36
F.2	Requirements on the HRPD Network as an IP-CAN	36
F.3	Information Flows	36
Annex G (Informative):	TEL-URI provisioning considerations for IMS emergency call back.....	37
Annex H (Normative):	IMS emergency services using UTRAN and E-UTRAN radio access network	38
H.1	General	38
H.2	UE specific behaviour	38
H.3	High Level Procedures for IMS emergency calls.....	38
H.4	Location handling.....	39
H.5	Domain Priority and Selection Rules for Emergency Call Attempts	39
Annex I (normative):	IMS Emergency Services Using HRPD/EPC Network.....	40
I.1	cdma2000 HRPD/EPC Options.....	40
I.2	Requirements on the HRPD/EPC Network as an IP-CAN.....	40
I.3	Information Flows	40
Annex J (informative):	Change history	41
History		42

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, TS 23.060 [2] describing GPRS (UTRAN), TS 23.401 [28], TS 23.060 [2]; TS 23.402 [29] describing EPS (UTRAN and E-UTRAN); TS 23.234 [7] describing 3GPP/WLAN Interworking; TS 23.271 [5] that covers location services and TS 23.216 [31] and TS 23.237 [32] describing Single Radio Voice Call Continuity for IMS Emergency session. TS 25.301 [6] contains an overall description of the UMTS Terrestrial Radio Access Network TS 36.300 [30] contains an overall description of the Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN). Other non-3GPP specifications that are related to the IMS emergency services include 3GPP2 cdma2000 HRPD IP-CAN, as specified in 3GPP2 X.S0060 [25] when the UE is connected to a PDS core network and 3GPP2 X.S0057-A [39] when the UE is connected to an EPC core network.

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 RFC 4676: "Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) Option for Civic Addresses Configuration Information".
- [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".
- [22] Void.
- [23] ANSI/J-STD-036-B: "Enhanced Wireless 9-1-1, Phase 2".
- [24] 3GPP2 X.S0002-0: "MAP Location Services Enhancements".
- [25] 3GPP2 X.S0060: "HRPD Support for Emergency Service".
- [26] 3GPP TS 22.003: "Circuit Teleservices supported by a Public Land Mobile Network (PLMN)".
- [27] 3GPP TS 22.228: "Service requirements for the Internet Protocol (IP) multimedia core network subsystem; Stage 1".
- [28] 3GPP TS 23.401: "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access".
- [29] 3GPP TS 23.402: "Architecture enhancements for non-3GPP accesses".
- [30] 3GPP TS 36.300: "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2".
- [31] 3GPP TS 23.216: "Single Radio Voice Call Continuity (SR VCC); Stage 2".
- [32] 3GPP TS 23.237: "IP Multimedia Subsystem (IMS) Service Continuity; Stage 2".
- [33] 3GPP TS 24.301: "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access".
- [34] 3GPP TS 26.114: "IP Multimedia Subsystem (IMS); Multimedia telephony; Media handling and interaction".
- [35] 3GPP TS 32.260: "Telecommunication management; Charging management; IP Multimedia Subsystem (IMS) charging".

- [36] ETSI TS 181 019 V2.0.0: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Business Communication Requirements".
- [37] ETSI TS 182 024 v.2.1.1: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Hosted Enterprise Services; Architecture, functional description and signalling".
- [38] ETSI TS 182 025 v.2.1.1: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Business trunking; Architecture and functional description".
- [39] 3GPP2 X.P0057-A v1.0: "E-UTRAN - eHRPD Connectivity and Interworking: Core Network Aspects".

Editor's note: The above document cannot be formally referenced until it is published by 3GPP2, at which time it will be designated as X.S0057-A rather than X.P0057-A.

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].

Charging Data Record: Record generated by a network element for the purpose of billing a subscriber for the provided service. See TS 32.260 [35] for further details.

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] or J-STD-036 [23].

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]).

Local regulation: Condition defined by the authority whose legislation applies where the emergency service is invoked.

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 Location Server or contain an integrated Location Server 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.

Location Server (LS): General term for the entity responsible for obtaining the location of the UE (e.g. GMLC see 3GPP TS 23.271 [5], MPC see 3GPP2 X.S0002 [24] or SLP see OMA AD SUPL [15]).

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.

Operator policy: Condition set by operator.

Private Numbering Plan: According to ETSI TS 181 019 [36], a numbering plan explicitly relating to a particular private numbering domain.

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 or in an LRF, provides the proper PSAP destination address to the E-CSCF for routing the emergency request. It can interact with a LS to manage ESQK allocation and management, and deliver location information to the PSAP.

For the purposes of the present document, the following terms and definitions given in TS 24.229 [19] apply:

Private Network Traffic

NOTE: All traffic from UEs having registered a contact bound to a public user identity receiving hosted enterprise services, is private network traffic.

Public Network Traffic

3.2 Abbreviations

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

CDR	Charging Data Record
CLF	Connectivity session Location and repository Function
E-CSCF	Emergency-CSCF
EATF	Emergency Access Transfer Function
ECS	Emergency Call Server
ESQK	Emergency Service Query Key
ESRK	Emergency Service Routing Key
ESRN	Emergency Service Routing Number
HRPD	High Rate Packet Data
LRF	Location Retrieval Function
LRO	Last Routing Option
LS	Location Server
MPC	Mobile Positioning Centre
PDS	Packet Data Subsystem
PSAP	Public Safety Answering Point
RDF	Routing Determination Function
SET	SUPL Enabled Terminal
SLP	SUPL Location Platform
SUPL	Secure User Plane for Location
VPC	VoIP Positioning Centre

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], TS 22.228 [27] 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. The URIs allowed to resolve to emergency services may be subject to local regulation in the serving network.
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 if required by local regulation.

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.

Subject to local regulation or operator policy, the network and the UE shall support the same authentication and security methods for an emergency service request as for non-emergency requests.

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, when the UE has roamed out of its home network, emergency services shall not be provided by the home network and shall be provided in the roamed-to network if the roamed-to network supports emergency sessions. If 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. If 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 centres and PSAPs may be connected to the PSTN, CS domain, PS domain or any other packet network.

12. The architecture shall enable emergency centres and PSAPs to request a PSAP call back session to a UE with which the Emergency centres or PSAPs had an emergency session, if the UE is registered (i.e. containing valid credentials). PSAP call back is subject to local regulation.

NOTE 1: PSAP call back sessions are treated as normal calls.

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. The network (e.g. in the E-CSCF) shall prevent the sending of the information of the users, such as public user identifiers and the location information, to the PSAP if explicitly requested by the user (i.e. request on session by session basis), and local regulation requires the operator to provide privacy to the user..

22. Void.

NOTE 2: 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 or cdma2000 HRPD and contains a limited number of emergency service categories. Therefore, an improved capability may need to be developed for IMS Emergency calls.

23. Void.

24. Subject to operator policy, the architecture shall allow an emergency session to be initiated by a trusted AS on behalf of a user that is not roaming.

25. Subject to local regulation, for non-roaming subscribers the network shall apply normal routing procedures for private network traffic even if that is marked as emergency session.

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, supplementary services interactions) 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.
- When a UE using public network traffic initiates an emergency session, the P-CSCF is the IMS network entity, which is responsible to detect the request for emergency session. The P-CSCF then forwards the request to E-CSCF in the same network, unless authentication and security procedures (see principle #7) require the request to be forwarded to the S-CSCF in the same network.

NOTE 3: If a UE generating private network traffic performs an emergency registration, a subsequently initiated emergency session is using public network traffic.

- The P-CSCF serving the emergency call is the IMS network entity which may retrieve the location identifier from the IP-CAN. For emergency sessions initiated by a trusted AS on behalf of a non-roaming subscriber, the AS may provide the location identifier.

- 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

When a UE performs an emergency registration, barring and roaming restrictions are ignored. The implicit registration set of the Public User Identifier used for emergency registrations shall contain an associated TEL-URI.

NOTE: Annex G provides recommendations for the provisioning of TEL-URI(s) in the IMS subscription for the purposes of IMS emergency sessions.

When a call is initiated to a PSAP from a UE without credentials, the E-CSCF shall derive a non-dialable callback number where required by local regulation (e.g. see Annex C of ANSI/J-STD-036 B [23]).

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 where required by local regulation.

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.
- If a trusted AS is used for the emergency session, the AS may provide the location identifier.
- When an emergency session is coming from a private network, it is assumed that the private network includes the initial location information in the request to establish an emergency session and subsequent location information as requested.

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 type of emergency service requested and to the type of emergency service requested and to the current location of the UE or to a default PSAP/Emergency Centre. The access dependent variations of this approach are described in the respective access specific annexes, for the cases where the UE is using GPRS (UTRAN), EPS (UTRAN and E-UTRAN), 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 via PS domain or via BGCF/MGCF through the CS domain. 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]).

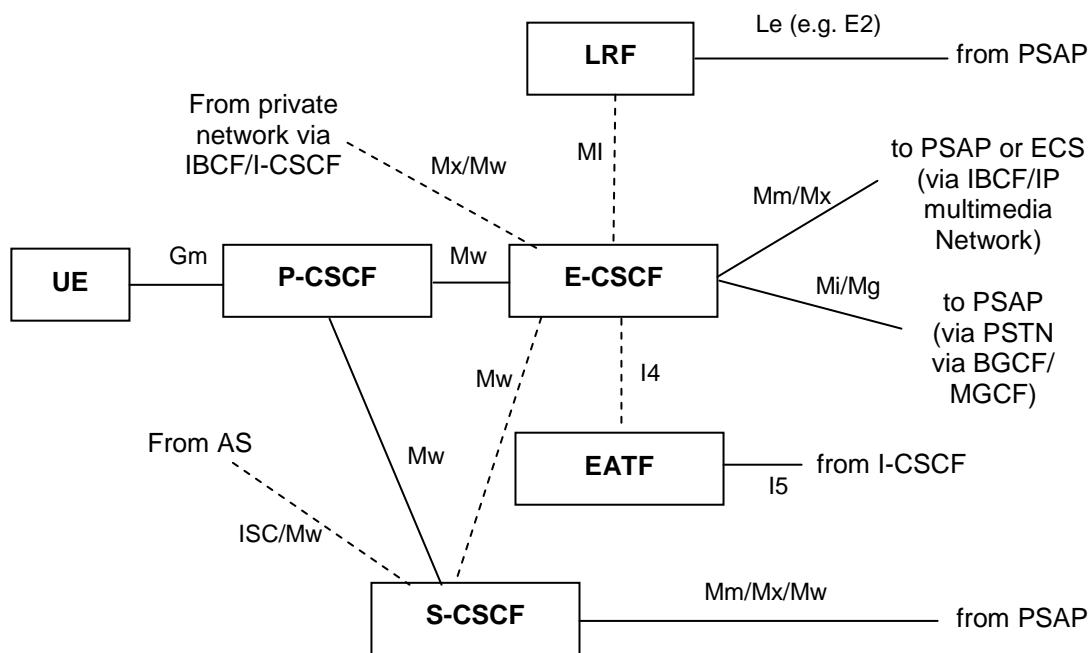
If the IP-CAN is a GPRS (UTRAN) network, the detailed procedures are described in TS 23.060 [2]. If the IP-CAN is an EPS (UTRAN and E-UTRAN) network, the detailed procedures are described in TS 23.401 [28], TS 23.060 [2] and TS 23.402 [29].

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.

**Legend:**

Dashed lines: optional interfaces

Figure 5.1: E-CSCF in reference architecture

NOTE 1: P-CSCF, EATF and E-CSCF are always located in the same (serving) network; this is the visited network when the UE is roaming. For emergency session initiation, the S-CSCF and AS are only applicable for non-roaming cases.

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

NOTE 3: Based on operator policy, the E-CSCF can 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, Mg, Mi, MI, Mm, Mx and I4 reference points to connect to other IMS entities and other IP Networks.

I4 is a reference point between an E-CSCF and an EATF. See TS 23.237 [32].

I5 is a reference point between an I-CSCF and an EATF. See TS 23.237 [32].

6 Functional description

6.1 UE

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

- Attempt the emergency call in CS domain, if capable.
- Handle a 380 (Alternative Service) response with the type set to "emergency" e.g. 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.
- A registered Public User Identifier. If the UE performed an emergency registration using a temporary Public User Identifier then the UE should not use the temporary Public User Identifier to initiate the emergency session. The selected Public User Identifier shall be part of an implicit registration set that includes a TEL-URI.

NOTE 3: The UE can be preconfigured with information to select the appropriate Public User Identifier if more than one Public User Identifier is provisioned in the UE.

- 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 Public User Identifier, if available.
- GRUU, if available.

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

NOTE 4: 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 registration indication 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 operator 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 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.
- Alternatively, for non-roaming subscribers, the P-CSCF may forward an emergency session to an S-CSCF if so instructed by operator policy or local regulation.

NOTE: This can be for example the case if the P-CSCF recognizes that an emergency session was not received via a security associations for a UE previously authenticated with digest type proxy authentication.

- Do not apply emergency session detection if requested using private network traffic and forward the session to the S-CSCF, except if operator policy requires the P-CSCF to detect emergency session requests and treat detected emergency session requests as if they are part of public network traffic.
- For UEs without credentials, forward the equipment identifier to the E-CSCF that was received from the UE.
- 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 Public User Identifier used for an emergency registration.
- 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 or an S-CSCF.
- If the UE does not have credentials, a non-dialable callback number shall be derived where required by local regulation (e.g. see Annex C of J-STD-036 [23]).
- 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 local regulation, the E-CSCF may send the contents of the P-asserted ID or UE identification to the LRF.
- Based on operator policy, the E-CSCF may route the emergency IMS call to ECS for further call process.
- For supporting SRVCC, see TS 23.237 [32] and TS 23.216 [31], the E CSCF forwards the session establishment request to the EATF in the serving IMS network for anchoring.
- Generation of CDRs.

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 LS, 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 LS 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 regulation or operator policy of the serving system.

NOTE 1: The value of the emergency registration time is subject to local regulation and can be subject to roaming agreements.

The emergency registration shall be handled separately from the normal IMS registrations, and not affect the registration status of the user.

When an S-CSCF receives a session initiated by a non-roaming subscriber marked as emergency session from a P-CSCF, the S-CSCF:

- performs caller authentication in the same way as for any other sessions;
- if required, uses filter criteria to route to AS;
- and forwards the request to an E-CSCF.

When an S-CSCF receives a session marked as emergency session from an AS, the S-CSCF:

- if required, uses filter criteria to route to other ASs;
- and forwards the request to an E-CSCF.

NOTE 2: The AS can initiate an emergency request on behalf of a non-roaming user, can convert private network traffic to public network traffic, or can interpret a number in private numbering plan and detect that the request is for emergency session.

6.2.5 Void

6.2.6 Emergency Access Transfer Function (EATF)

The EATF provides IMS emergency session continuity which is specified in TS 23.237 [32].

6.2.7 Interrogating-CSCF

I-CSCF supports IMS emergency session continuity which is specified in TS 23.237 [32].

6.2.8 AS

An AS can be involved in emergency session handling (e.g. for emergency sessions made via hosted enterprise services ETSI TS 182 024 [37], or for AS initiated session).

Dependent on the service provided by the AS, if the AS is the first point that identifies an IMS emergency session, then the AS shall provide the following emergency session handling functions:

- Detect an emergency session establishment request.
- Verify that the UE is not roaming.
- Optionally obtain location.
- Prioritize the emergency session.
- Provide in the session establishment request the TEL URI associated to the public user identity, in global format, if known and not already present.
- Check the validity of the caller TEL URI if provided by the UE.
- Mark the request as an emergency session request.

NOTE: If the AS converts a request marked as private network traffic to public network traffic and the request is marked by the AS as emergency session, the AS routes the request back to the S-CSCF, which will forward the request towards a public PSAP. If a request is targeted to a private PSAP, then it is marked as private network traffic and normal routing procedures in the IMS network will deliver the request to its target, possibly with priority handling if mandated by local regulations.

6.2.9 HSS

In the course of an emergency registration, the HSS shall not apply any barring condition and/or roaming restriction associated with the Public User Identity received in the emergency registration request.

The emergency registration shall be handled separately from the normal IMS registrations, and not affect the registration status of the user.

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.

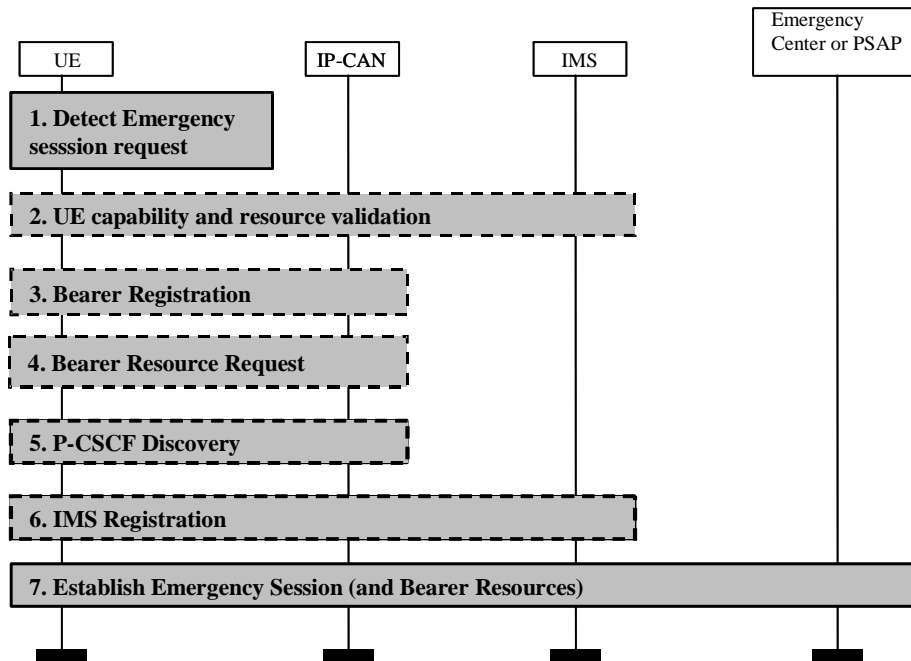


Figure 7.1: Terminal Detected Emergency Calls

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. The IP-CAN may support a UE indication that this request is for an emergency service.
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 indication. The implicit registration set of the SIP URI used in the emergency registration request 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 regulation or operator policy of the serving system. The subsequent registration flows are like any other registration with the considerations defined in clauses 6.2.4 and 6.2.9.

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 clause 7.4 and skip step 7.

7. 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. If the UE has performed emergency registration, the UE shall use an emergency 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 operator 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:
 - if a dialled number is available, attempt to initiate a call to the dialled number in the CS domain as follows:
 - for systems based on TS 24.008 [13], the ME and/or (U)SIM may contain emergency numbers according to clause 10.1.1 in TS 22.101 [8], which may include the dialled number:
 - if the dialled number is not on the ME and/or (U)SIM, the UE will fail to recognize the dialled number as an emergency number and so the UE will attempt a normal call (i.e. TS11, see TS 22.003 [26]), and the MSC Server will recognise the number and route it to a local PSAP;
 - if the dialled number is on the ME and/or (U)SIM the UE will indicate the emergency call type (i.e. TS12, see TS 22.003 [26]);
 - for CS system that do not support emergency call handling procedures (e.g. as described by TS12 in TS 22.003 [26] for systems based on TS 24.008 [13] or in systems providing access to IM CN subsystem using a cdma2000 network, for example) a normal call is made;
 - if a dialled number is unavailable, attempt to initiate an emergency call in the CS domain (e.g. as described by TS12 in TS 22.003 [26] for systems based on TS 24.008 [13]); or
 - follow the procedure in clause 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. The P-CSCF in the visited PLMN forwards that request to an Emergency CSCF in the same network. The P-CSCF in the home PLMN for a non-roaming UE may forward that request to a Serving CSCF or to an Emergency CSCF in the same network, based on local regulation or operator policy. The E-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.

If the AS detects that this is a request to establish an emergency session, the AS shall handle the request as specified in clause 6.2.8 and forward the request marked as an emergency services request to the S-CSCF.

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.

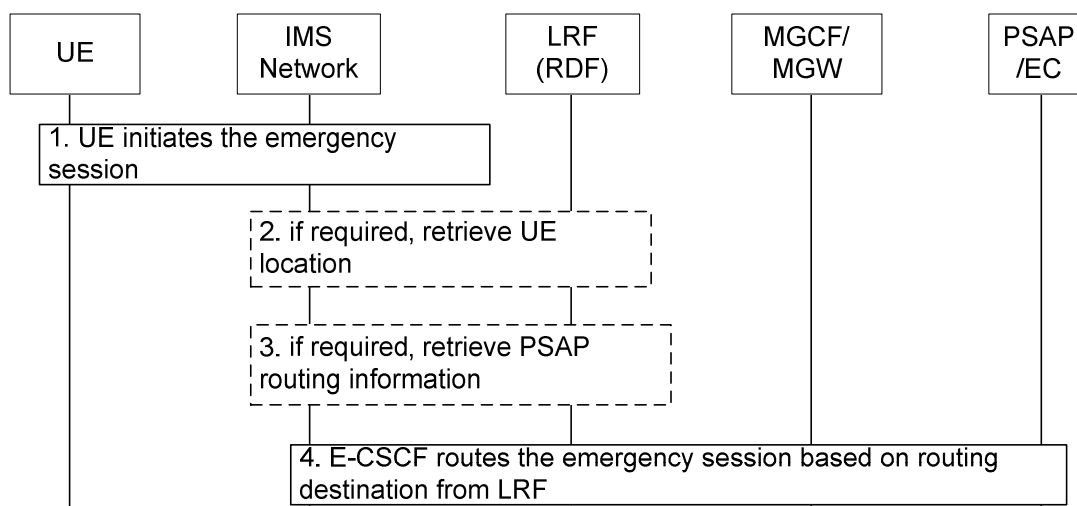


Figure 7.2: Emergency Session Establishment procedure with using LRF/RDF

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 indication in the emergency registration request. This indication may be used 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.

P-CSCF handles the registration requests with an emergency indication 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 regulation or operator policy in the serving system. The subsequent registration flows are like any other registration with the considerations defined in clauses 6.2.4 and 6.2.9.

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.

The UE shall follow the requirements in TS 22.101 [8] for domain priority and selection when UE attempts to make an emergency call.

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 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:

- When a UE using public network traffic initiates an emergency session, 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 operator 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 registration, 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].

Handling of emergency sessions detected by an AS is specified in clause 6.2.8.

For the case where the emergency session is provided via the interconnect from a private network (as defined in ETSI TS 182 025 [38]), the following procedures apply:

- For private network traffic where operator policy allows so, do not apply emergency session detection and forward the session according to normal procedures.
- Otherwise emergency sessions within the IMS are routed to the PSAP via the E-CSCF.

Upon receiving an initial request for an emergency session, 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 regulation, 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.

Where required by local regulation, the E-CSCF shall derive a non-dialable callback number to include as the UE's identity in the session establishment request and the location/routing request (e.g. see Annex C of J-STD-036 [23]).

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. Emergency call and call back feature interactions are handled as specified in TS 22.101 [8].

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. Emergency call and call back feature interactions are handled as specified in TS 22.101 [8].

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. Emergency call and call back feature interactions are handled as specified in TS 22.101 [8].

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.

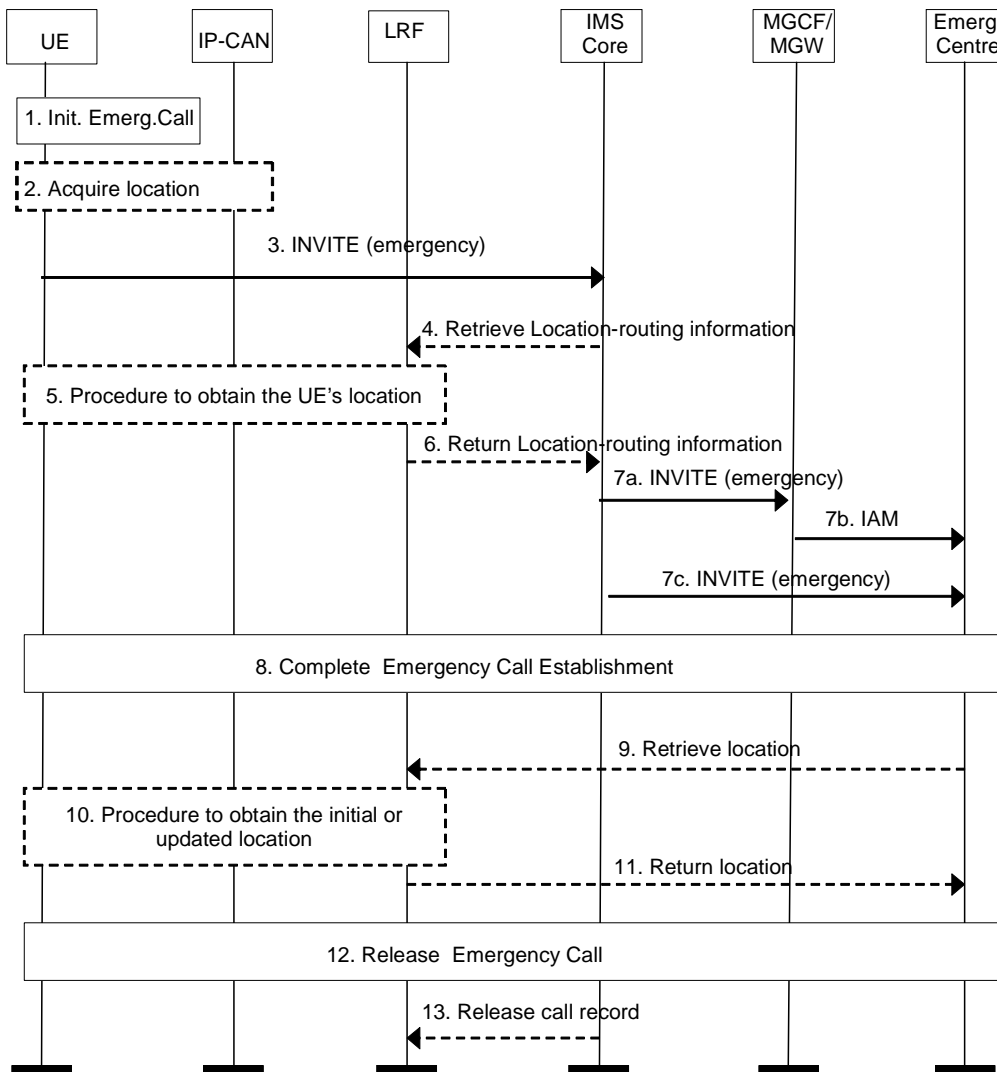


Figure 7.6-1: Handling of location information in IMS emergency calls

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

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.

NOTE: Clause 9.2.5 of TS 23.271 [5] describes the Mobile Originated Location Request procedure for Location Services for I-WLAN.

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].

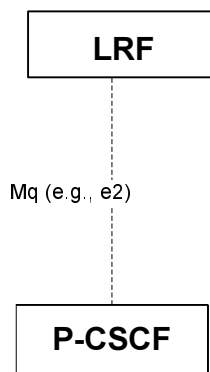


Figure C.1: Additional P-CSCF interface for fixed broadband access

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 RFC 4676 [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

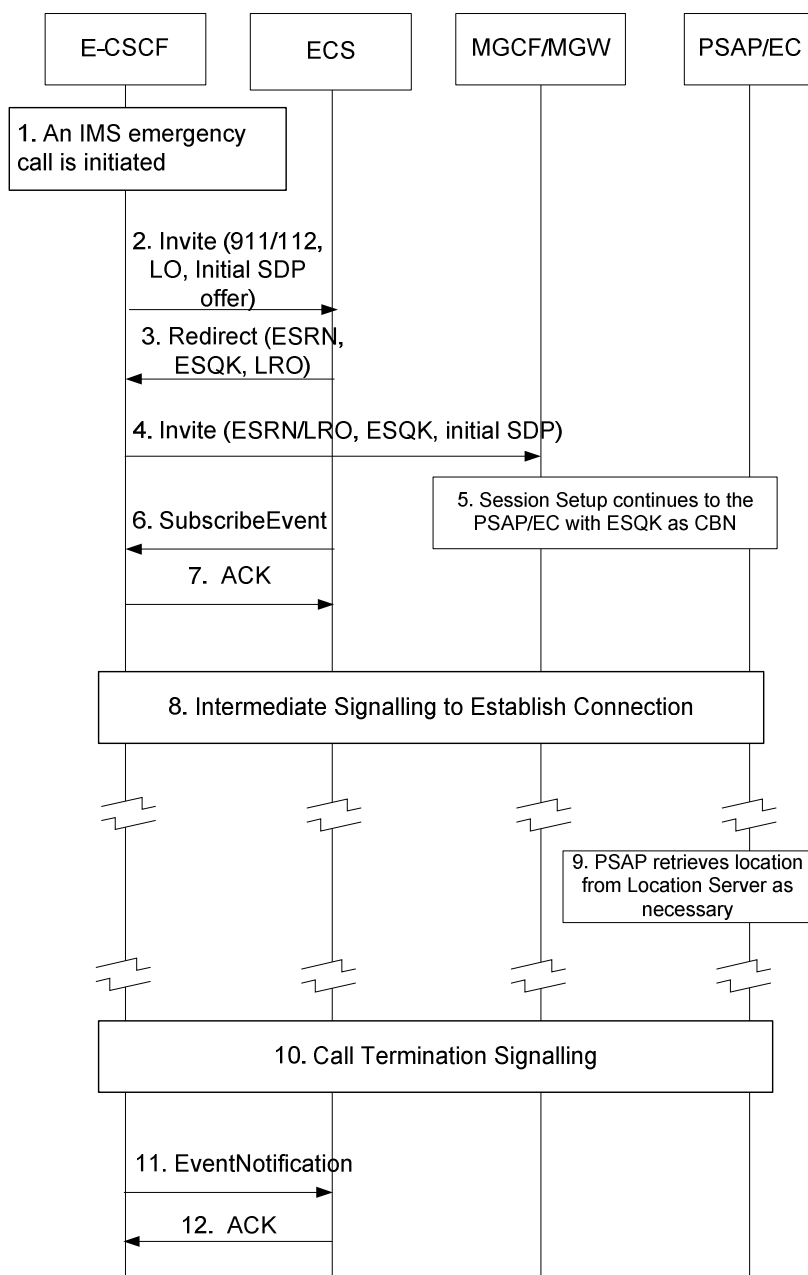


Figure D.1

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 Event Notification 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

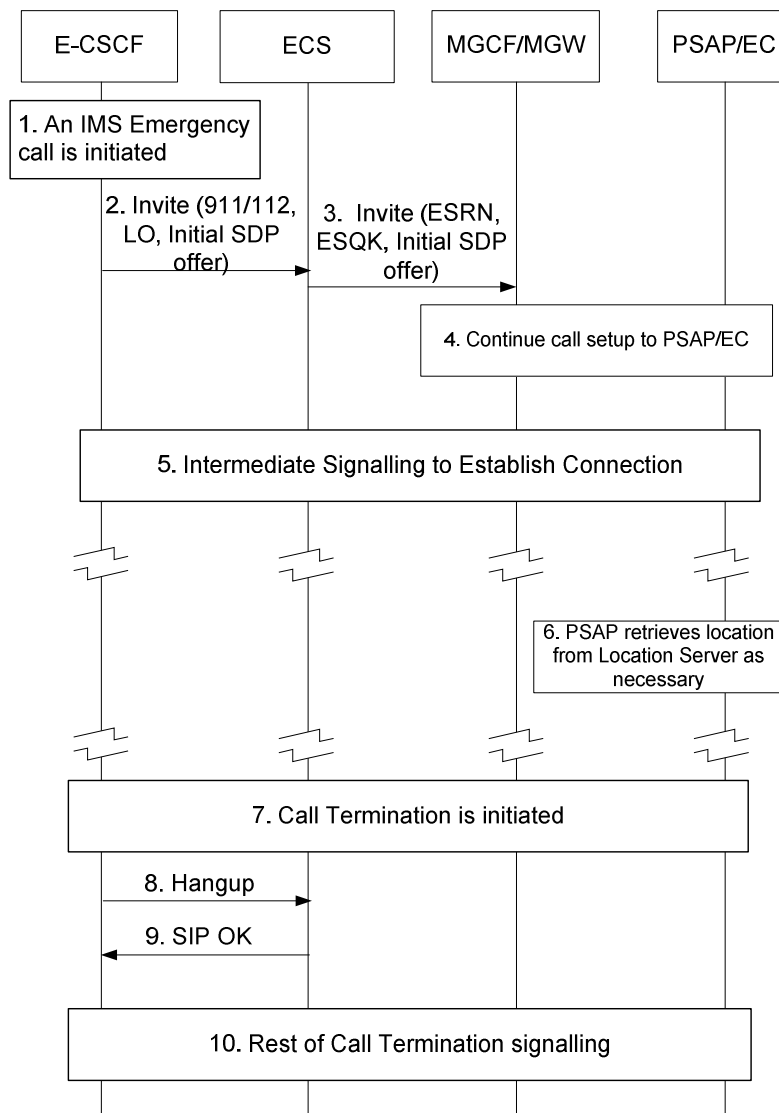


Figure D.2

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 hang-up 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 (UTRAN)	X	X	X
I-WLAN	X	X	X
Fixed Broadband	X	X	X
cdma2000 HRPD/PDS	X	X	X
cdma2000 HRPD/EPC	X	X	X
EPS (UTRAN and E-UTRAN)	X	X	X

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 (normative): IMS Emergency Services Using HRPD/PDS Network

F.1 cdma2000 HRPD/PDS Options

The following options from the normative sections of this TS are applicable in cdma2000 HRPD systems with a PDS core network:

- 1) Clause 7.1.1, step 4 "The IP-CAN may support a UE indication that this request is for an emergency service".

The following options from the normative sections of this TS are not applicable in cdma2000 HRPD/PDS systems:

- 1) Clause 4.1 "The P-CSCF serving the emergency call is the IMS network entity which may retrieve the location identifier from the IP-CAN".

F.2 Requirements on the HRPD Network as an IP-CAN

For an emergency call over HRPD, the requirements on the IP-CAN are specified in 3GPP2 X.S0060 [25].

F.3 Information Flows

The informational flows for emergency calls over HRPD are provided in 3GPP2 X.S0060 [25].

Annex G (Informative): TEL-URI provisioning considerations for IMS emergency call back

In order to support emergency call-back from the PSTN or CS Domain:

- For a single or multiple device subscription that contain both a SIP-URI and TEL-URI in at least one implicit registration set for each device (including subscriptions that share SIP-URIs and TEL-URIs between devices), IMS emergency sessions can already be supported. If the user registers with a temporary public user identity (e.g. the subscription has a device containing a USIM) ensure that a TEL-URI is provisioned in the same implicit registration set as the temporary public user identity.
- For existing subscriptions that do not contain TEL-URIs (e.g. because none of the devices in the subscription are allowed to use a TEL-URI in normal originations) then provision a new TEL-URI in the subscription and either:
 - Place the TEL-URI in one of the existing implicit registration sets that are assigned to all devices and set the TEL-URI to barred; or
 - Create a new implicit registration set for all devices containing a SIP-URI and TEL-URI used only by a device for emergency registration and set both URIs to barred.
- For a multiple device subscription that has TEL-URIs for some devices but has one or more devices that are not assigned an implicit registration set containing a TEL-URI (e.g. because these devices in the subscription are not allowed to use a TEL-URI in normal originations), the existing TEL-URIs in the subscription cannot be shared between all devices for the purposes of IMS emergency sessions. For the devices that are not assigned a TEL-URI, create a new implicit registration set containing a SIP-URI and TEL-URI used only by a device for emergency registration and set both URIs to barred.

Annex H (Normative): IMS emergency services using UTRAN and E-UTRAN radio access network

H.1 General

This annex includes additional requirements and clarifications when the IP-CAN is a PS Domain supporting UTRAN and E-UTRAN radio access network.

If a PLMN supports other emergency numbers than those listed in TS 22.101 [8], and the UE is connected to the PLMN using UTRAN or E-UTRAN radio access network, then such emergency numbers shall be provided to the UE via the mobility management procedures as described in TS 24.301 [33] and TS 24.008 [13].

For registration requests received from an emergency PDN connection, the P-CSCF shall reject any IMS registration which is not for the emergency purpose.

H.2 UE specific behaviour

For the specific case of an emergency call over EPS or GPRS the UE shall use the following procedures:

- A UE shall establish an emergency PDN connection and perform an IMS emergency registration before initiating a UE detectable emergency session via UTRAN or E-UTRAN.
- A UE shall not establish an emergency PDN connection if the UE initiated a non UE detectable emergency session and is subsequently informed by the network that the ongoing session is an emergency session.

NOTE 1: If SRVCC is required in the network, an operator could download the local emergency numbers to avoid non UE detectable emergency sessions since UTRAN and E-UTRAN will not be able to identify emergency SRVCC handling without an emergency PDN connection.

- If the UE initiates a non UE detectable emergency session, and the session initiation request is rejected by the P-CSCF with an indication that this is an emergency session, the UE shall select a domain according to the requirements for domain priority and selection in clause H.5 and attempt an emergency call on that domain (i.e. a UE detectable emergency session or a CS emergency call).
- If the UE has not been authenticated in the PS domain, the UE shall initiate an IMS emergency session establishment without registration according to clause 7.4.
- The UE shall include the latest available Cell Global Identification (CGI) in the IMS emergency request establishing the emergency call.

NOTE 2: When using UTRAN, the UE is not always able to read the current cell identity and in some cases the UE can be connected to several cells simultaneously.

- If the UE is required to include an equipment identifier (according to clauses 4.1 and 6.1) the equipment identifier shall be the IMEI.
- the speech Codexes defined for MTSI as specified in TS 26.114 [34] shall also be supported for the IMS emergency calls.

H.3 High Level Procedures for IMS emergency calls

For the high level procedures (as described in clause 7.1.1) the following statements apply for UE detected emergency calls when PS domain with UTRAN and E-UTRAN access is used:

- the bearer registration to the IP-CAN is the PS attach procedure;
- the IP-CAN bearer resource is the PDP context for GPRS and EPS Bearer for EPS, and the TS 23.060 [2] and the TS 23.401 [28] respectively describe how to indicate that the request is for emergency;
- the release of reserved bearer resources is the release of a PDP context or an EPS Bearer.

For the high level procedures (as described in clause 7.1.2) the following statements apply for Non UE detectable emergency calls when PS domain with UTRAN and E-UTRAN access is used:

- The P-CSCF rejects the session initiation request with an indication that this is an emergency session; or
- the P-CSCF allows the session initiation request to continue and the E-CSCF informs the UE that it is an emergency session. Such a session will not use emergency PDN connections and will not have SRVCC or SRVCC for IMS emergency session support.

H.4 Location handling

The applicable location solutions are specified in TS 23.271 [5] for control plane and SUPL 2.0 (OMA AD SUPL [15], OMA TS ULP [16]) for user plane. For SUPL, SUPL Initiation Function using UDP/IP (OMA AD SUPL [15]) shall be supported by the SET.

H.5 Domain Priority and Selection Rules for Emergency Call Attempts

This clause details the domain priority and selection (see clause 7.3) for UE that attempts to make an emergency call for UTRAN and E-UTRAN radio access networks based on the UE attach status to CS or PS domains and the network support for IMS emergency and IMS voice over PS.

The following table (Table H.1) defines these rules based on the UE (last 2 columns) for different initial conditions (first 4 columns) when an emergency call is initiated and when the UE is not in limited service state.

Table H.1: Domain Selection Rules for emergency call attempts for UTRAN and E-UTRAN radio access networks

	CS Attached	PS Attached	VoIMS	EMS	First EMC Attempt	Second EMC Attempt
A	N	Y	Y	Y	PS	CS if available and supported
B	N	Y	N	Y	PS or CS	PS if first attempt in CS CS if first attempt in PS
C	N	Y	Y or N	N	CS if available and supported	
D	Y	N	Y or N	Y or N	CS	PS if available and EMS is "Y"
E	Y	Y	Y	Y	Follow rules in TS 22.101 [8] which say to use the same domain as for a non-EMC	PS if first attempt in CS CS if first attempt in PS
F	Y	Y	Y or N	N	CS	
G	Y	Y	N	Y	CS	PS

EMC = Emergency Call.

VoIMS = Voice over IMS over PS sessions support as indicated by IMS Voice over PS session supported indication as defined in TS 23.401 [28] and TS 23.060 [2].

EMS = IMS Emergency Services supported as indicated by Emergency Service Support indicator as defined in TS 23.401 [28] and TS 23.060 [2].

Annex I (normative): IMS Emergency Services Using HRPD/EPC Network

I.1 cdma2000 HRPD/EPC Options

The following options from the normative sections of this TS are applicable in cdma2000 HRPD systems with an EPC core network:

- 1) Clause 7.1.1, step 4 "The IP-CAN may support a UE indication that this request is for an emergency service".

The following options from the normative sections of this TS are not applicable in cdma2000 HRPD/EPC systems:

- 1) Clause 4.1 "The P-CSCF serving the emergency call is the IMS network entity which may retrieve the location identifier from the IP-CAN".

I.2 Requirements on the HRPD/EPC Network as an IP-CAN

For an emergency call over HRPD/EPC, the requirements on the IP CAN are specified in 3GPP2 X.S0057-A [39].

I.3 Information Flows

The informational flows for emergency calls over HRPD are provided in 3GPP2 X.S0057-A [39].

Annex J (informative): Change history

Change history								
Date	TSG #	TSG Doc.	CR	Rev	Cat	Subject/Comment	Old	New
2010-06	SA#48	SP-100344	0173	-	F	Adding back requirements for PSAP call back indicator in release 10	9.4.0	10.0.0
2010-09	SA#49	SP-100546	0177	6	B	Alternative emergency session handling in non-roaming cases	10.0.0	10.1.0
2010-09	SA#49	SP-100557	0179	-	F	Deletion of the last emergency IMPU	10.0.0	10.1.0
2010-12	SA#50	SP-100676	0181	1	A	Adding IMS Emergency support for HRPD with EPC IP-CAN	10.1.0	10.2.0
2010-12	SA#50	SP-100691	0183	1	F	Terminology correction	10.1.0	10.2.0
2011-01	-	-	-	-	-	Update of LTE logo to LTE-Advanced logo	10.2.0	10.2.1
2011-03	SA#51	SP-110063	0185	1	A	PSAP call back handling in S-CSCF	10.2.1	10.3.0
2011-09	SA#53	SP-110455	0188	1	A	Correction of emergency procedures	10.3.0	10.4.0
2011-12	SA#54	SP-110730	0196	1	A	Correction of emergency procedures	10.4.0	10.5.0
2011-12	SA#54	SP-110737	0200	1	F	Clarification on S-CSCF handling when receiving emergency session from AS.	10.4.0	10.5.0
2011-12	SA#54	SP-110869	0203	5	A	Clarifications on non UE detectable emergency call	10.4.0	10.5.0
2012-06	SA#56	SP-120234	0214	1	A	Requirement Alignment for call back and emergency registration	10.5.0	10.6.0

History

Document history		
V10.3.0	March 2011	Publication
V10.4.0	October 2011	Publication
V10.5.0	January 2012	Publication
V10.6.0	July 2012	Publication