3GPP TS 23.167 V15.4.0 (2018-12)

Technical Specification

3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects;
IP Multimedia Subsystem (IMS) emergency sessions
(Release 15)

Keywords
LTE, UMTS, PS, emergency, IMS

3GPP

Postal address

3GPP support office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet
http://www.3gpp.org

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 and IM emergency services for eCall. 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] describing EPS (UTRAN and E-UTRAN); TS 23.402 [29] describing Non 3GPP access (WLAN) to EPC; TS 23.271 [5] that covers location services; TS 23.216 [31] and TS 23.237 [32] describing Single Radio Voice Call Continuity (SRVCC) and Dual Radio Voice Call Continuity (DRVCC) for IMS Emergency session, TS 23.292 [45] describing the use of IMS services when using CS access for the media bearer and TS 23.501 [48] and TS 23.502 [49] describing support of emergency services and location for 5GS. 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); and TS 38.300 [50] contains an overall description of the Next Generation Radio Access Network (NG-RAN). 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] Void.

[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.S0057-C v1.0: "E-UTRAN - eHRPD Connectivity and Interworking: Core Network Aspects".

[40] NENA 08-002, Version 1.0 (i3): "NENA Functional and Interface Standards for Next Generation 9-1-1".

[41] 3GPP TS 23.122: "Non-Access-Stratum (NAS) functions related to Mobile Station (MS) in idle mode".

[42] 3GPP TS 26.267: "Digital cellular telecommunication systems (Phase 2+); Universal Mobile Telecommunication System (UMTS); eCall data transfer; In-band modem solution General description".

[43] 3GPP TS 23.328: "P Multimedia (IM) Subsystem Sh interface; Signalling flows and message contents".

[44] 3GPP TS 33.203: "3G security; Access security for IP-based services".

[45] ATIS-0700028: "Location Accuracy Improvements for Emergency Calls".

[46] 3GPP TS 23.292: "IP Multimedia Subsystem (IMS) centralized services".

[47] IEEE Std 802.11-2012: "IEEE Standard for Information technology--Telecommunications and information exchange between systems Local and metropolitan area networks--Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications".

[48] 3GPP TS 23.501: "System Architecture for the 5G System; Stage 2".

[49] 3GPP TS 23.502: "Procedures for the 5G System; Stage 2".

[50] 3GPP TS 38.300: "NR; Overall description; Stage-2".

[51] 3GPP TS 23.503: "Policy and Charging Control Framework for the 5G System; Stage 2".

[52] 3GPP TS 24.501: "Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3".

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.

NG-eCall (eCall Over IMS): A manually or automatically initiated IMS emergency call, from a vehicle, supplemented with a minimum set of emergency related initial data (MSD).

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 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

For the purposes of the present document, the following terms and definitions given in TS 23.401 [28] apply:

eCall Only Mode: See TS 23.401 [28].

For the purposes of the present document, the following terms and d efinitions given in TS 22.101 [8] apply:

eCall: See TS 22.101 [8].

Minimum Set of Data (MSD): See TS 22.101 [8].

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
CS	Circuit Switched
DRVCC	Dual Radio Voice Call Continuity
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
MSD	Minimum Set of emergency related Data
PDS	Packet Data Subsystem
PSAP	Public Safety Answering Point
RDF	Routing Determination Function
SET	SUPL Enabled Terminal
SLP	SUPL Location Platform
SRVCC	Single Radio Voice Call Continuity
SUPL	Secure User Plane for Location
URN	Uniform Resource Name
VPC	VoIP Positioning Centre
WLAN	Wireless LAN

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, a nomadic access and a WLAN access to EPC or untrusted non-3GPP access to 5GC (using procedures for Un-trusted access to EPC (respectively 5GC)).

2a. Emergency numbers and associated types or URN information received via WLAN (for access to EPC) are only used for detecting emergency calls in the same country, if permission from PLMN selected in 3GPP access was received (see TS 23.401 [28] and TS 23.060 [2] for EPC access).

NOTE 1: Some features described in this clause do not apply for emergency session set-up over WLAN access to EPC or to 5GC. The limitations are documented in Annex J and Annex L.

2b. Emergency numbers and associated types received using a list as described in TS 24.008 [13] are only used for detecting emergency calls in the same country. The UE can obtain these numbers and associated types via mobility management procedures as described in TS 24.008 [13], TS 24.301 [33] and TS 24.501 [52]. The associated types consist of a limited number of emergency service categories from which a limited number of URNs can be derived.

2c. Emergency numbers and associated URN information received using a list as described in TS 24.301 [33] are only used when they are valid. The validity of these numbers and associated URN information is specified in TS 22.101 [8] clause 10.4.1 (i.e. the serving network indicates whether this list is valid in the country or only in the PLMN). The UE can obtain these numbers and associated URN information via mobility management procedures as described in TS 24.301 [33] and TS 24.501 [52].

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.

9a. 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 and if the serving IMS has indicated support for anonymous IMS emergency sessions as part of the IMS registration failure, the UE shall attempt an anonymous emergency session. If the IMS registration fails and if the serving IMS has not indicated support for anonymous IMS emergency sessions as part of the IMS registration failure, the UE may attempt an anonymous IMS emergency session.

NOTE 2: UEs compliant with pre-Rel-14 versions of this specification are unable to interpret this indication and ignore the indication. Such UEs might attempt an anonymous IMS emergency session or proceed according to Annex H.5.

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 to a UE with which the Emergency centres or PSAPs had an emergency session. The serving network of the UE shall use the appropriate call termination procedures e.g. IMS if the UE is available for voice over PS, or ICS if the user is available over CS. PSAP call back is subject to local regulation.

NOTE 3: PSAP call back sessions are treated as normal calls.

NOTE 4: Subject to local regulation, any supported media can be used during a call back attempt from a PSAP.

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 5: TS 24.008 [13] contains a procedure to provide local emergency numbers for UMTS and GPRS access but the procedure is not applicable to cdma2000 HRPD and contains a limited number of emergency service categories.

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.

26. When a call is established with a PSAP that supports voice only, voice media is supported and GTT if required by local regulation or operator policy.

27. When a call is established with a PSAP that supports voice and other media, voice, GTT and other media according to TS 22.101 [8] (e.g. video, session mode text-based instant messaging) can be used during an IMS emergency session if required by local regulation. This media may be used in addition to or instead of voice and/or GTT.

28. NG-eCall is a variant of IMS emergency services and follows the same principles, architecture, and procedures as other emergency services over IMS.

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 6: While in the home network, forwarding of an emergency session to the S-CSCF is only expected over a non-emergency registration.

- 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 P-CSCF serving the emergency call is the IMS network entity which may receive additional caller related identifier(s) from the IP-CAN (e.g. IP-CAN level's subscriber ID). If required by local regulation, these additional identifier(s) shall be forwarded by the IMS network to the emergency control centre/PSAP for those UEs that have not been authenticated by IMS network and are requesting to establish an emergency session,

- 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 via or BGCF, IBCF or IP multimedia network based on location information and additionally other information such as type of emergency service in the request.

- As a regional option where the emergency centre/PSAP is connected to the IMS of another network (e.g. TTC spec), emergency sessions may be routed over Inter-IMS Network to Network Interface between two IM CN subsystem networks.

- The architecture shall allow for compliance with other regional regulations (i.e. ATIS and NENA specs in North America region) in which the originating network shall have the ability to route an emergency call via an IBCF to an emergency services network.

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.

NOTE: For untrusted non-3GPP access to 5GC, provided location information can only correspond to the UE IP address seen by the N3IWF and used for traffic destined towards the UE.

- 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.

- For WLAN access, the LRF may query HSS for NPLI if the UE is not roaming. In some regions, for example in the North American region [45], if the BSSID of the serving WLAN is available, the LRF may query a database subject to national regulations and operator policies for the dispatchable location associated with the BSSID of the WLAN Access Point.

- 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), 5GS (NG-RAN), fixed broadband access, WLAN access to EPC or untrusted non-3GPP access to 5GC 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:

- Except for emergency services over WLAN access to EPC or untrusted non-3GPP access to 5GC, 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].

- In the case that the IP-CAN receives a request to establish bearer resources for emergency services, the IP-CAN may provide additional identifier(s) to IMS network (e.g. IP-CAN level's subscriber ID).
- 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] and TS 23.060 [2] and in Annex H. If the IP- CAN corresponds to WLAN access to EPC, the detailed procedures are described in TS 23.402 [29] and in Annex J. If the IP-CAN is a 5GS (NG-RAN) network, the detailed procedures are described in TS 23.502 [49] and in Annex H. If the IP- CAN corresponds to untrusted non-3GPP access to 5GC, the detailed procedures are described in TS 23.502 [49] and in Annex L.

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

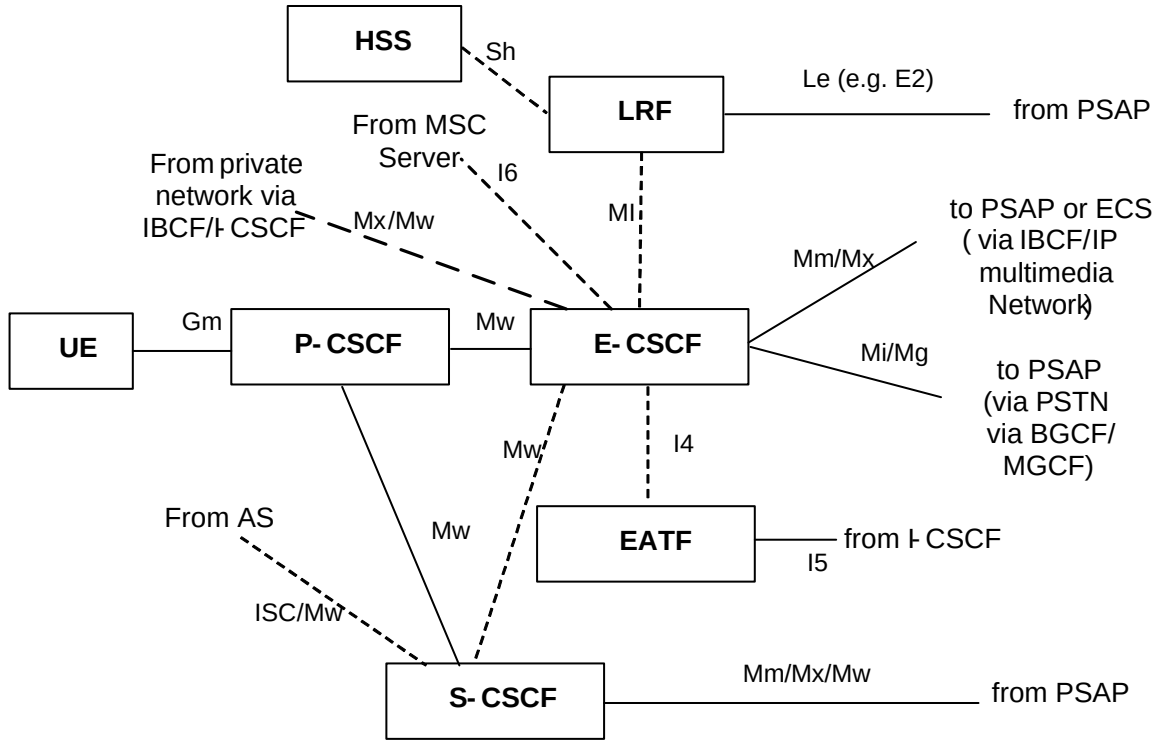
4.5 Media

- When the call is established with a PSAP that supports voice only, voice and subject to local regulation, GTT media is allowed during the IMS emergency session.
- When the call is established with a PSAP that supports voice and other media, subject to UE and network support for the other media and local regulation, voice, GTT and other media according to TS 22.101 [8] can be used during the IMS emergency session.
- For sessions with a PSAP that supports voice and other media, media can be added, modified or removed during the IMS emergency session (e.g. adding video to a voice call) per media negotiation in TS 23.228 [1].
- When a PSAP that supports voice and other media attempts to add media, the media shall be added if accepted by the UE.

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, MSC Server enhanced for ICS, 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, Ml, 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].

I6 is a reference point between an MSC Server enhanced for ICS and E-CSCF. See TS 23.292 [46].

Sh is a reference point between LRF and HSS. See TS 23.328 [43].

6 Functional description

6.1 UE

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

- In the case of NG-eCall, the IMS emergency session establishment request may be invoked either automatically without user input or manually via user input.

- 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.

- UE may support the GIBA procedure defined in TS 24.229 [19] as part of the emergency IMS registration procedure.

- In case of emergency IMS registration failure the UE shall be able to interpret the indication, if provided by the serving IMS, whether anonymous IMS emergency sessions are supported in the serving IMS. If the serving IMS has indicated support, the UE shall proceed with an anonymous IMS emergency session, otherwise it proceeds according to clause H.5.

NOTE 1: UEs compliant with pre-Rel-14 versions of this specification are unable to interpret this indication and ignore the indication. Such UEs might attempt an anonymous IMS emergency session or proceed according to clause H.5.

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

NOTE 2: "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 an equipment identifier in the request to establish an emergency session when the UE supports SRVCC as specified in TS 23.237 [32].

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

NOTE 3: 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].

- For NG-eCall, where transfer of the MSD is not acknowledged by the PSAP, the UE shall fall back to the in-band transfer of the MSD, as in CS domain defined in TS 26.267 [42].

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 service 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 4: 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 service indication.

- For an NG-eCall an eCall indication including whether eCall is automatic or manual.

- 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 described in clause 7.1.2.

NOTE 5: 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.
- May query IP-CAN for additional subscriber related identifier(s).
- 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 and when the request is received over a non-emergency registration, 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 association 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.
- For UEs without credentials and subjected to local regulation, forward the additional subscriber related identifier(s) received from IP-CAN to the E-CSCF.
- 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 service 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.
- Upon IMS registration failure the P-CSCF may indicate to the UE whether anonymous IMS emergency sessions are supported.

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 and/or DRVCC, 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.
- For an NG-eCall and if an LRF/RDF is not deployed, the E-CSCF may use an indication of an automatic eCall or a manual eCall to assist routing of an emergency session establishment request.
- For supporting emergency session request from MSC Server enhanced with ICS, see TS 23.292 [46]. E-CSCF follows the same procedure as defined for handling emergency session request from P-CSCF.

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. For WLAN access, and for non-roaming UEs, if the LRF is configured then it may interact with HSS to provide an NPLI before interacting with the RDF. In some regions, for example in the North American region, ATIS-0700028 [45], if the BSSID of the serving WLAN is available, the LRF may query a database subject to national regulations and operator policies for the dispatchable location associated with the BSSID of the WLAN Access Point.

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 as normal IMS registrations with the following considerations:

- Upon emergency registration:
  - If a normal registration for the user does not exist, the S-CSCF shall download corresponding user profile from HSS to ensure that HSS allocates S-CSCF name to this subscriber and the registration status is set to UNREGISTERED.
  - Otherwise, S-CSCF shall ensure that the registration status of the user is not changed in the HSS.
- Upon deregistration or expiration of the last normal session:
  - If an emergency registration for the user still exists, the S-CSCF shall ensure that the HSS keeps S-CSCF name allocated to this subscriber and the registration status is set to UNREGISTERED.
- Upon expiration of an emergency registration:
  - If a normal registration for the user still exists, the S-CSCF shall ensure that the registration status of the user is not changed in the HSS.
  - Otherwise, the S-CSCF can either de-register the user in HSS or keep the registration status of the user unchanged in the HSS.

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.

NOTE 3: Reception of a session initiation request marked as an emergency session from a P-CSCF and/or an AS by the S-CSCF is only expected over a non-emergency registration.

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).

NOTE 1: The participation of an AS in emergency session handling is only expected over a non-emergency registration.

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 2: 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 with the considerations defined in clause 6.2.4.

6.2.10 Media Gateway Control Function (MGCF)

For NG-eCall MGCF handles the emergency session as normal emergency call establishment.

NOTE: The MGCF does not forward the initial MSD, if received in the emergency session request.

6.2.11 MSC Server enhanced with ICS

The MSC Server enhanced with ICS may provide interworking mechanisms to support emergency call using CS media bearer and using IMS for routing/handling the emergency call toward PSAP. From the view point of E-CSCF, MSC

Server enhanced with ICS behaves like a P-CSCF. Further details on MSC Server procedure are defined in TS 23.292 [46].

6.2.12 IBCF

- Forward emergency session establishment requests.
- Prioritize the emergency session based on operator policy.

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.

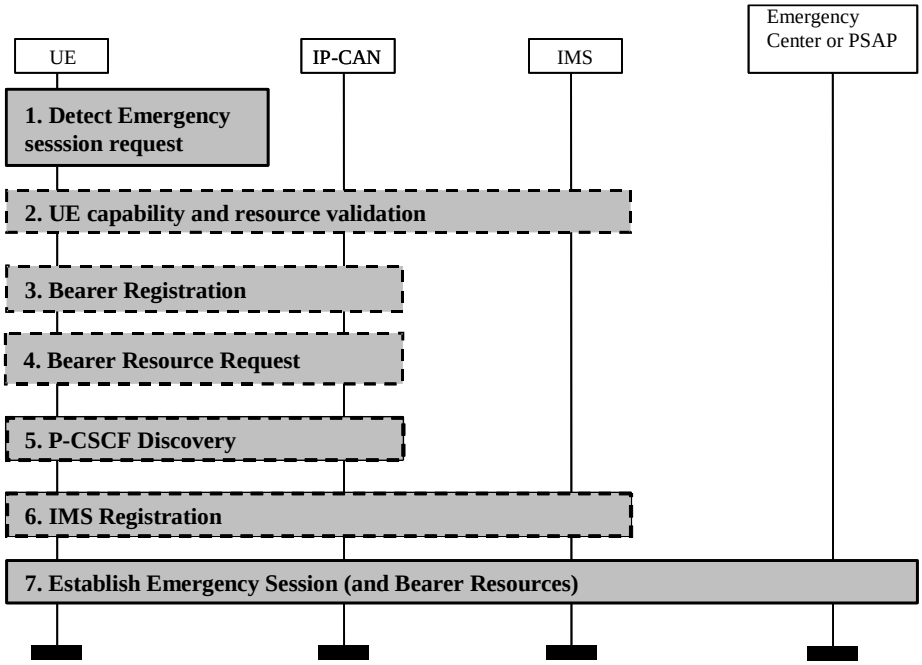


Figure 7.1: Terminal Detected Emergency Calls

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 used by the UE when the UE performs a non emergency registration shall contain an associated TEL-URI that is used to call back the UE.

   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 service indication, or the eCall type of emergency service indication in the case of eCall 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:
  - select a domain for the emergency session;
  - if the PS domain is selected, follow the procedure in clause 7.1.1;
  - for systems based on TS 24.008 [13], if the CS domain is selected and a dialled number is available, attempt a normal call (i.e. TS 11, see TS 22.003 [26]) using the dialled number if:
    - an emergency service information is included by the P-CSCF with either a country specific emergency subservice type (see TS 24.229 [19]) or a emergency subservice type (see TS 24.229 [19]) that does not map into an emergency service category for the CS domain; or
    - no emergency service information is included by the P-CSCF;

- for systems based on TS 24.008 [13], if the CS domain is selected, attempt an emergency call (i.e. TS 12, see TS 22.003 [26]) if:
  - a dialled number is not available; or
  - an emergency service information is included by the P-CSCF with no emergency subservice type or a emergency subservice type (see TS 24.229 [19]) that maps into an emergency service category for the CS domain;
- if the CS domain is selected and for CS systems 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 prior attempting the call in the CS domain the UE receives a list of local emergency numbers, the UE may verify if and recognizes the dialled number is an emergency number and if verified, 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.

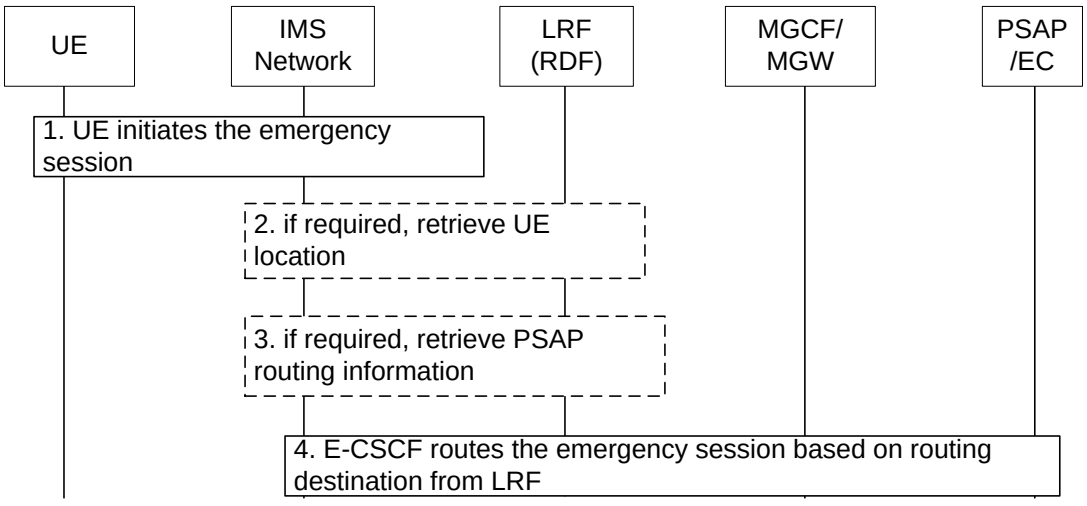


Figure 7.2: Emergency Session Establishment procedure with using LRF/RDF

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. For WLAN access, and for non-roaming UEs, if the LRF is configured then it may interact with HSS to provide an NPLI. In some regions, for example in the North American region, ATIS-0700028 [45], if the BSSID of the serving WLAN is available, the LRF may query a database subject to national regulations and operator policies for the dispatchable location associated with the BSSID of the WLAN Access Point.

NOTE 1: The details of the LRF querying a national database (e.g. in North America) are outside the scope of this specification.

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 2: 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 or UPF 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. In the case of NG-eCall, the UE shall include the eCall type of emergency service (automatic or manual) 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 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 and if not disallowed by applicable domain selection rules. 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 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, the UE's location and any indication of an eCall.
- 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, including any additional subscriber related identifier(s) received from P-CSCF.

- 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. Based on local regulation, P-CSCF may retrieve additional subscriber related identifier(s) from IP-CAN and forward those identifiers to E-CSCF.

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/routeing 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].

7.5.4 PSAP supporting NG-eCall

It is assumed that the PSAP supporting the NG-eCall shall be able to receive and verify the consistency of the initial MSD within the initial SIP INVITE.

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.

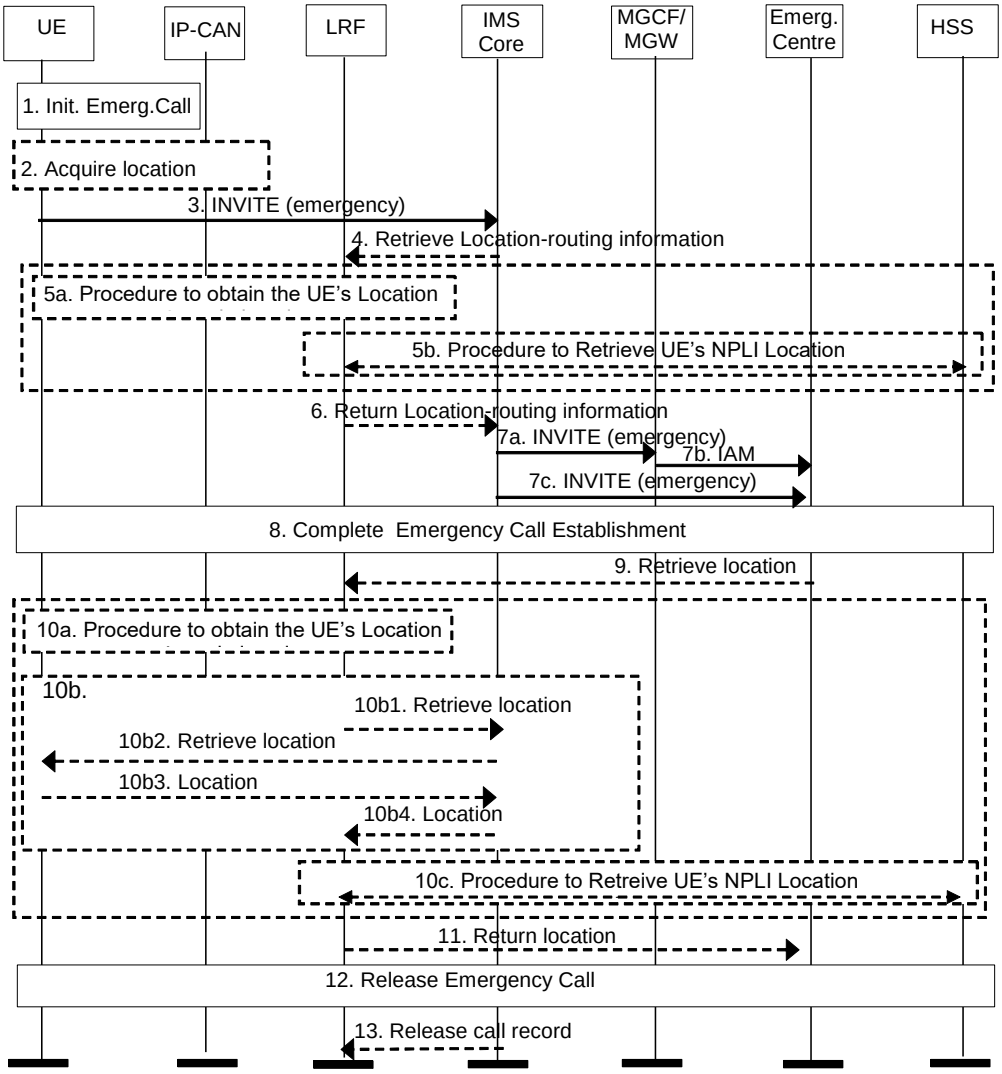


Figure 7.6-1: Handling of location information in IMS emergency calls

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.

   5a. 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.

   5b. If configured to provide an NPLI for WLAN access, and if the UE is not roaming, the LRF queries HSS for every access the LRF is configured for. The LRF issues a separate query for every access. If the LRF cannot obtain an NPLI, it shall invoke procedure 5a.

   The LRF may invoke an RDF to convert the location information received in step 4 or obtained in step 5a 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 5a.

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. Depending on the access type, UE location is determined as follows:

    10a. For non WLAN-access and optionally for WLAN access, the LRF determines the target UE's location using one of the means listed in step 5a above. The LRF may use the correlation information received in step 9 to retrieve information about the UE that was stored in step 5a.

    10b. For WLAN access, the LRF may use the correlation information received in step 6 to send a request to the IMS core to retrieve a UPLI from the UE. The IMS core uses the emergency call signalling channel for

that purpose. Steps 10b1 to 10b4 depict this procedure. If UPLI is not available when the request comes to the UE (e.g. due to insufficient time), and UPLI cannot be returned, the UE may also provide UPLI once, when available by executing step 10b3 following step 8.

10c. For WLAN access, and if the LRF is configured to provide an NPLI for WLAN access, and if the UE is not roaming, the LRF queries HSS for every access the LRF is configured for. The LRF issues a separate query for every access. If the LRF cannot obtain an NPLI, it shall invoke procedure 10a.

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 10a 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 5a.

7.6.2 Void

7.6.3 Void

7.7 Transfer of MSD for eCall

7.7.1 MSD Transfer/Acknowledgement during Session Establishment with PSAP supporting NG-eCall

Figure 7.7.1-1 illustrates a high level call flow for an interworking scenario between a UE and a PSAP supporting NG-eCall.

This scenario occurs, when the UE detects that the NG-eCall is supported by the IP-CAN.

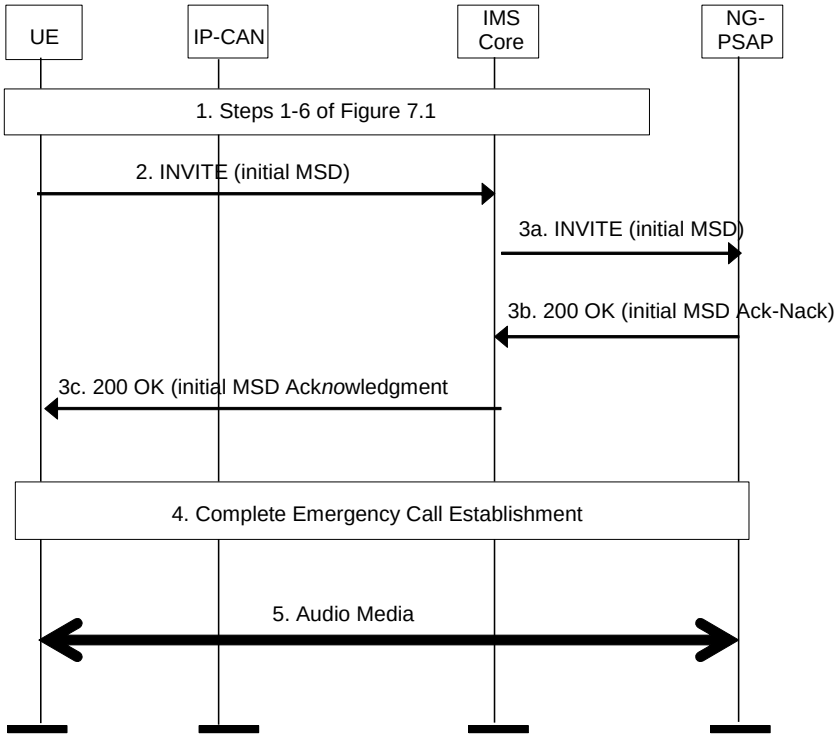


Figure 7.7.1-1: NG-eCall Scenario with PSAP supporting NG-eCall

1. The UE performs steps 1 to 6 of the procedure shown in Figure 7.1.
2. The UE sends an initial emergency SIP INVITE to the IMS core. The SIP INVITE shall contain the initial MSD and the eCall type of emergency service indicator (automatic, manual).

3a. The IMS core routes the SIP INVITE towards the appropriate PSAP.

NOTE 1: Routing within the IMS core is based on the UE location and the eCall type of emergency service indication, but not on the content of the initial MSD. The PSAP may use also location data contained within the initial MSD.

3b. The PSAP verifies the correctness of the initial MSD and returns a SIP 200 OK to the IMS core. The SIP 200 OK explicitly includes a positive or negative acknowledgement for the initial MSD.

3c. The IMS core proxies the SIP 200 OK to the UE.

4. The emergency call establishment is completed. In addition to the transfer of MSD, media channels are established. In this case the emergency voice channel is established.
5. The established audio channel supports bidirectional voice communication,

7.7.2 MSD Transfer/Acknowledgement during Session Establishment with a PSAP Not supporting NG-eCall (inband means)

Figure 7.7.2-1 illustrates a high level call flow for an interworking scenario between a UE and a PSAP via the CS domain.

This scenario may occur in the case, when PS access is available, but the UE does not detect that the NG-eCall is supported by the IP-CAN and there is no CS access available. In this case, the UE shall establish a regular IMS emergency call.

A similar scenario may occur in the case, when the UE detects that the IP_C AN supports NG-eCall and initiates an NG eCall but the session is handled by a PSAP not supporting NG-eCall. The only exception would be step 2 and where the SIP INVITE shall contain the initial MSD and the eCall type of emergency service indicator (automatic, manual).

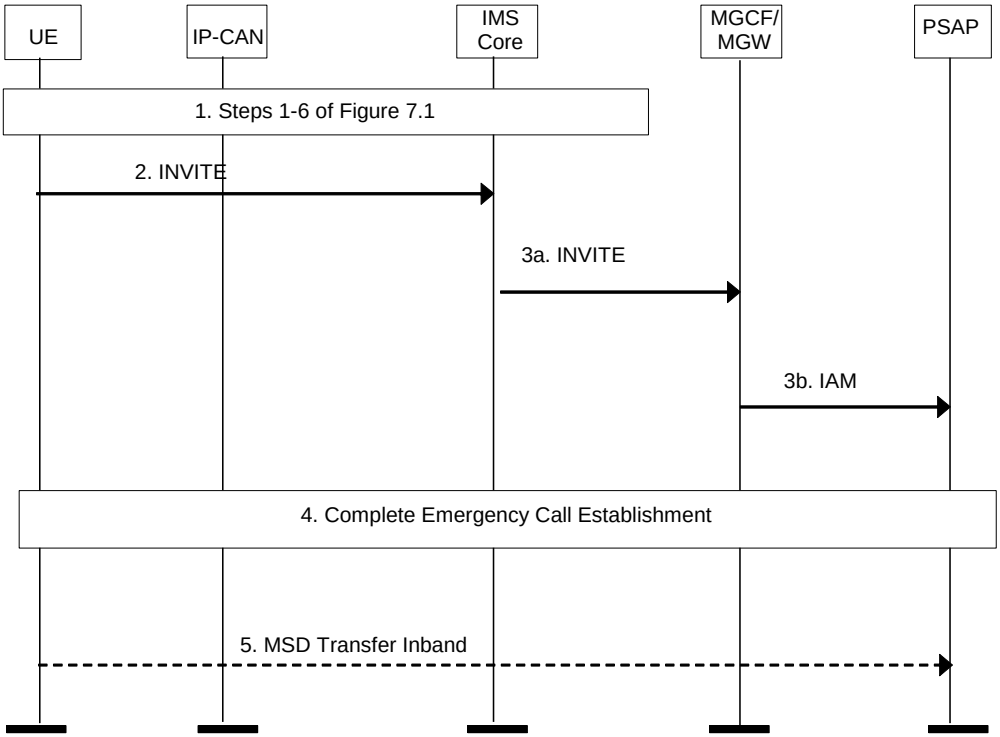


Figure 7.7.2-1: eCall Scenario with PSAP not supporting NG-eCall

1. The UE performs steps 1 to 6 of the procedure shown in Figure 7.1.
2. The UE sends an initial emergency SIP INVITE to the IMS core. The SIP INVITE shall be setup as follows:
   - if the UE has not received the "eCall supported" indication, the UE shall include the eCall type of emergency service indication (automatic, manual) and shall not include the initial MSD in case the PS access is available;
   - if the UE has received the "eCall supported" indication, the UE shall include the initial MSD and the eCall type of emergency service indicator (automatic, manual).
3. The IMS core routes the emergency SIP INVITE towards the appropriate PSAP. In this call flow, the appropriate PSAP is accessed over the MGCF and the CS domain after translating the eCall type of emergency service indication into the corresponding MSISDN.

3a. The SIP INVITE is sent to an MGCF/MGW for interfacing to the CS domain.

3b. The MGCF sends an IAM towards the appropriate PSAP for the emergency voice call.

4. The emergency voice call establishment is completed with a voice path only.
5. If the UE has sent the MSD in step 2 and did not receive acknowledgement for the initial MSD included in the SIP INVITE, or the UE did not send the MSD in step 2 the UE shall attempt to transfer the MSD to the PSAP via the eCall Inband Modem, as defined in TS 26.267 [42].

7.7.3 Transfer of an updated MSD

Figure 7.7.3-1 illustrates a high level call flow for transfer of an updated MSD in the case that the emergency centre or PSAP is accessed via the PS domain. The call flow is applicable following establishment of an emergency services session for eCall as described in clause 7.1.1 in which the initial MSD is transferred in the INVITE and prior to release of the emergency services session.

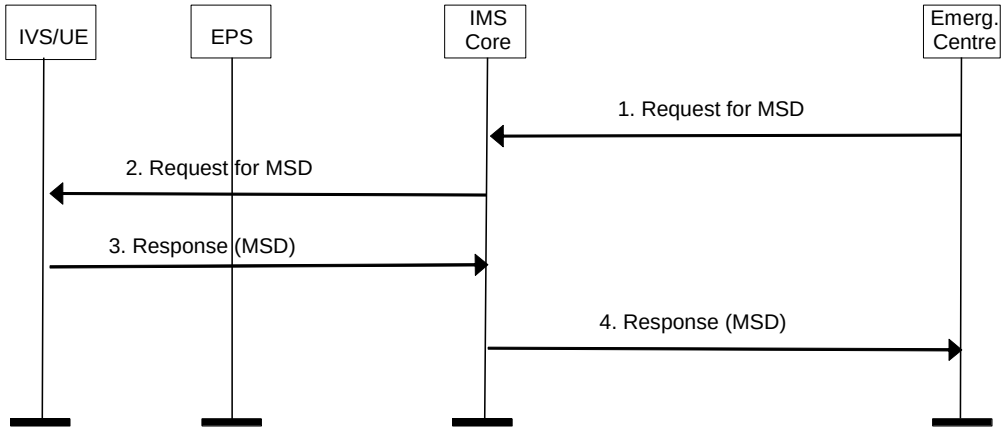


Figure 7.7.3-1: Sending an updated MSD for eCall

1. If the emergency centre or PSAP requires an MSD update, it may send a request for MSD to the IMS Core.
2. The IMS Core shall forward the request to the UE.
3. The UE shall send the most recent MSD to the IMS Core.
4. The IMS Core shall forward the MSD to the emergency centre or PSAP.

NOTE: Whether an acknowledgement message for the successful receipt of updated MSD by the PSAP is further provided to the UE is resolved in stage 3 level.

Annex A (informative):
Void

Annex B (informative):
Void

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 may have 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].

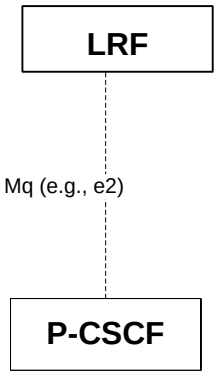


Figure C.1: Additional P-CSCF interface for fixed broadband access

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, if the UE supports such functionality. The access network may know the location of the access point where the UE is connected to. In this case, 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, if any, 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.

Alternatively, subject to operator policy, the S-CSCF may receive from the HSS a reference location of the user at registration, and insert it in the INVITE request, when network-provided location information is not already present. The reference location (e.g. line identification) is determined by the operator as part of the user profile.

NOTE: The reference location alternative is applicable to non nomadic services provided on fixed lines for emergency sessions that are routed through the S-CSCF (see clause 6.2.4). The reference location corresponds the physical location of the fixed line.

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

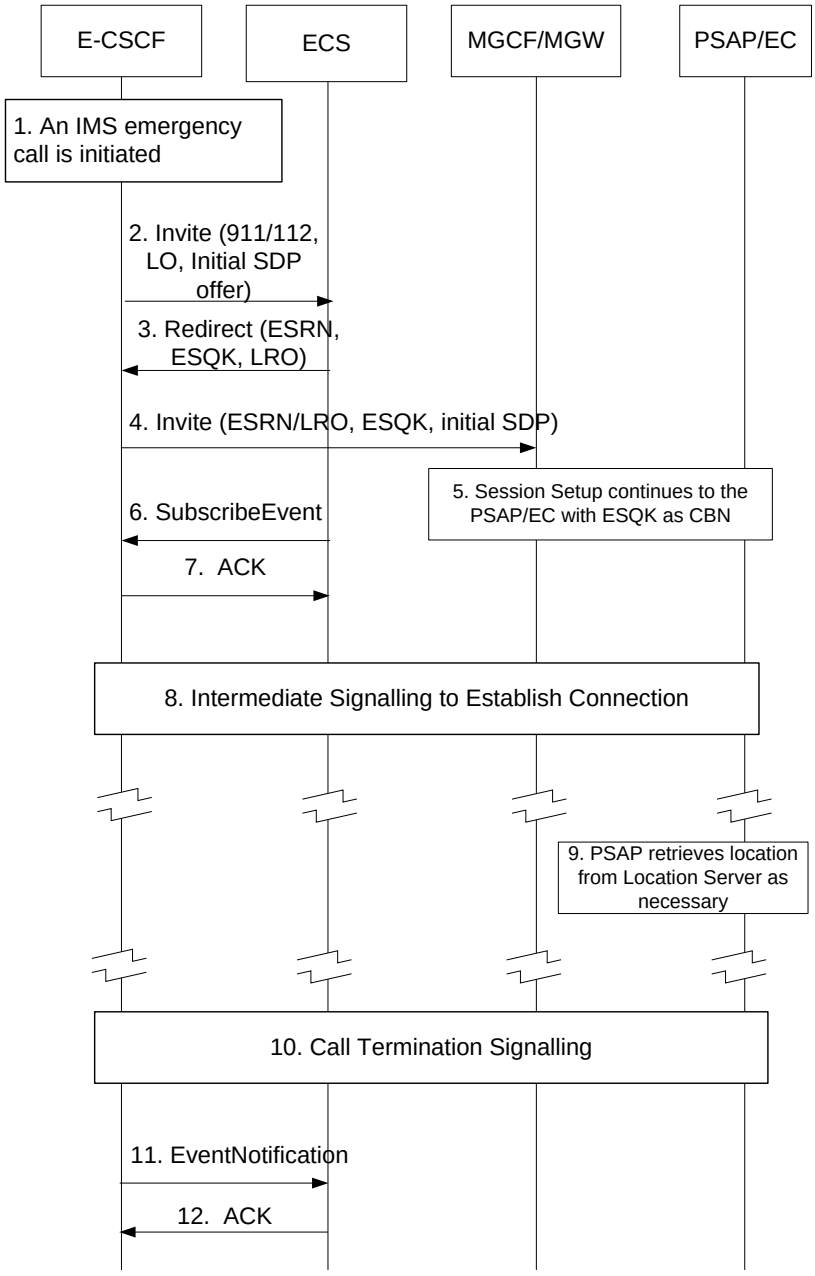


Figure D.1

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

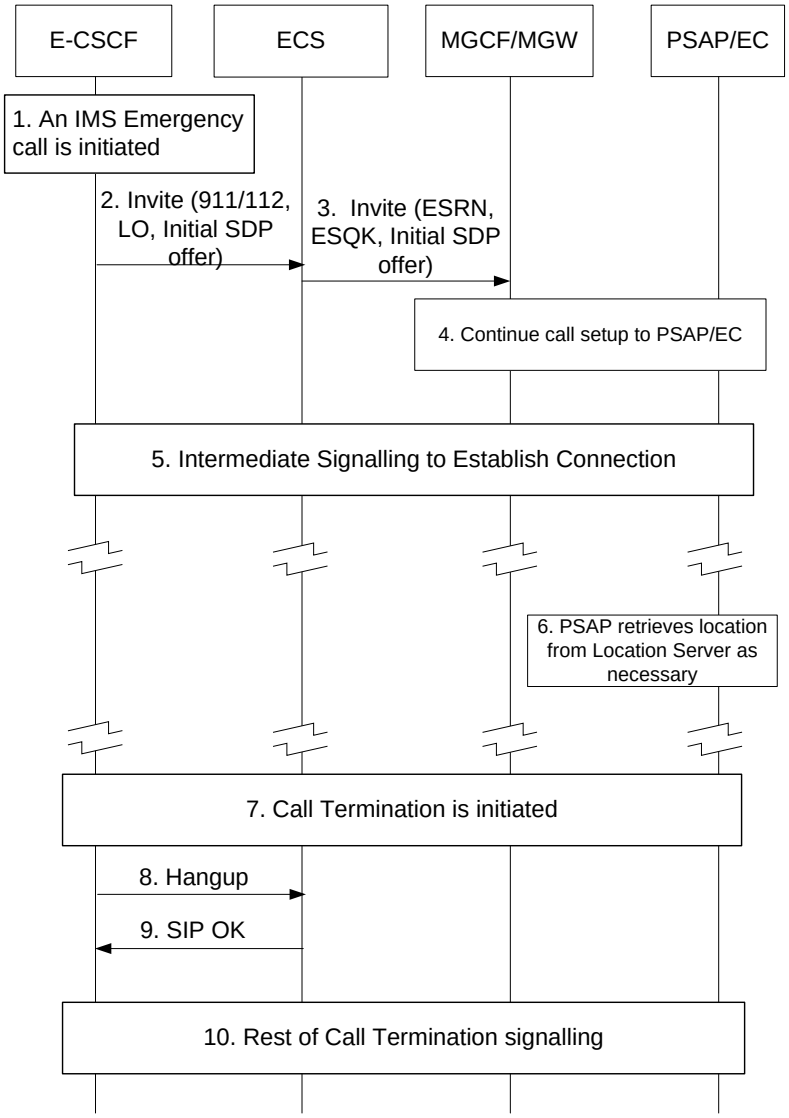


Figure D.2

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
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
WLAN access to EPS	X (NOTE 1)	X	-
5GS (NG-RAN)	X	X	X
untrusted non-3GPP access to 5GC	X (NOTE 1)	X	-
NOTE 1: Emergency Sessions use a normal access to EPC/5GC only in case of emergency sessions not detected by the UE and nevertheless served by the IMS network.			

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 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.

Annex H (normative): IMS emergency services using UTRAN, E-UTRAN and NG-RAN radio access network

H.1 General

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

If a PLMN supports other emergency numbers than those listed in TS 22.101 [8], the UE is connected to the PLMN using UTRAN, E-UTRAN or NG-RAN radio access network and the UE needs to know these other emergency numbers, then such emergency numbers shall be provided to the UE via the mobility management procedures as described in TS 24.301 [33], TS 24.008 [13] and TS 24.501 [52].

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

eCall is only supported with E-UTRAN and E-UTRA connected to 5GC. UE configured for eCall Only Mode can receive a PSAP call back for a limited duration following the termination of the eCall due to its specific mobility management procedures requirement as defined in TS 22.101 [8].

H.2 UE specific behaviour

For the specific case where the UE has selected to make an emergency call over EPS, GPRS or 5GS the UE shall use the following procedures:

- A UE shall establish an emergency PDN connection or emergency PDU session and perform an IMS emergency registration before initiating a UE detectable emergency session via UTRAN, E-UTRAN or NG-RAN.

- A UE shall not establish an emergency PDN connection or emergency PDU session 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 when applying the requirements in clause 7.1.2.

- A UE in 5GS shall not initiate establishment of an IMS emergency session over untrusted Non-3GPP access unless the emergency session could not be established via 3GPP access.

- 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.

- For the media supported during IMS emergency sessions in TS 22.101 [8] clause 10.4, media codec and format support is specified in TS 26.114 [34].
- UE shall only perform eCall procedure over IMS as specified in clause 7.7.1 when it detects the "eCall supported" indication as defined in TS 23.401 [28] and TS 23.501 [48].
- When PS access is available, but the UE does not detect the "eCall supported" indication as defined in TS 23.401 [28] and TS 23.501 [48], and there is no CS access available, the UE shall establish a regular IMS emergency call.
- If the broadcast indicators in an E-UTRA cell connected to 5G and EPC as defined in TS 23.501 [48] indicate only one core network (EPC or 5GC) supports emergency services then the UE shall register to the core network which supports emergency services when the UE initiates emergency services. If broadcast indicators indicate that both 5GC and EPC support emergency services then the UE initiates emergency services to either EPC or 5GC according to the UE implementation.

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, E-UTRAN or NG-RAN access is used:

- the bearer registration to the IP-CAN is the PS attach or PS Registration procedure;
- the IP-CAN bearer resource is the PDP context for GPRS, EPS Bearer for EPS and QoS Flow for 5GS, and TS 23.060 [2], TS 23.401 [28] and TS 23.501 [48] respectively describe how to indicate that the request is for emergency;
- the release of reserved bearer resources is the release of a PDP context, an EPS Bearer or a QoS Flow.

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, E-UTRAN or NG-RAN 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 an emergency PDN connection or emergency PDU session and will not have SRVCC or SRVCC for IMS emergency session support.

For the IMS Emergency Session Establishment without Registration (as described in clause 7.4), P-CSCF retrieves the additional subscriber related identifier(s) from IP-CAN via PCC in TS 23.203 [20] when PS domain with UTRAN and E-UTRAN access is used.

H.4 Location handling

The applicable location solutions are specified in TS 23.271 [5] for control plane with UTRAN and E-UTRAN access, in TS 23.501 [48] and TS 23.502 [49] for control plane with NG-RAN access and in 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.

If the operator policy requires network provided location using PCC-based solutions for the UE location (e.g. serving cell), the P-CSCF retrieves location information from the access network and includes it in the emergency service request, as described in TS 23.228 [1]. The UE location is marked as being network provided to distinguish it from location information that the UE provided.

If the operator policy requires network provided location using the LRF-based solution for the UE location (e.g. serving cell), the P-CSCF forwards the emergency request to E-CSCF. The E-CSCF retrieves location information from LRF as described in clause 6.2.2.

Operator policies in the P-CSCF and E-CSCF should be aligned to ensure that the E-CSCF doesn't attempt to retrieve location information from the LRF if network-provided location information is present in the initial emergency request.

However, as described in clause 6.2.2, the E-CSCF may request the LRF to retrieve additional location information (e.g. the UE's geographical location information).

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

This clause details the domain priority and selection (see clause 7.3) for UE that attempts to make an emergency session for UTRAN, E-UTRAN or NG-RAN 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 session is initiated and when the UE is not in limited service state.

For NG-eCall (eCall over IMS) domain selection in clause H.6 applies. This clause is not applicable for NG-eCall.

Table H.1: Domain Selection Rules for emergency session attempts for UTRAN, E-UTRAN or NG-RAN 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 - NOTE 7)
B	N	Y	N	Y	PS or CS if the emergency session includes at least voice. PS if the emergency session contains only media other than voice.	PS if first attempt in CS CS if first attempt in PS - NOTE 7)
C	N	Y	Y or N	N	PS if ESFB is "Y" (NOTE 5). Else CS or PS for another 3GPP RAT with EMS or ESFB set to "Y" if available and supported and if the emergency session includes at least voice. Else PS for another 3GPP RAT with EMS or ESFB set to "Y" if available and supported if the emergency session contains only media other than voice.	PS if first attempt in CS CS if first attempt in PS - NOTE 7)
D	Y	N	Y or N	Y or N	CS if the emergency session includes at least voice. PS if available and EMS or ESFB is "Y" and emergency session contains only media other than voice.	PS if available and EMS or ESFB is "Y"
E	Y	Y	Y	Y	If the emergency session includes at least voice, follow rules in TS 22.101 [8] which say to use the same domain as for a non-EMC (NOTE 2) PS if the emergency session contains only media other than voice.	PS if first attempt in CS CS if first attempt in PS
F	Y	Y	Y or N	N	PS if ESFB is "Y" (NOTE 5). Else PS for another 3GPP RAT with EMS if available and supported or CS, if the emergency session includes at least voice.	CS if first attempt in PS PS for another 3GPP RAT if available and supported and EMS or ESFB is "Y" if first attempt in CS.
G	Y	Y	N	Y	CS if the emergency session includes at least voice. PS if the emergency session contains only media other than voice.	PS

EMC = Emergency Session. EMC includes also normal calls initiated in the CS domain that are treated by the CS CN as emergency calls.
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], TS 23.060 [2] and TS 23.502 [49].
EMS = IMS Emergency Services supported as indicated by Emergency Service Support indicator as defined in TS 23.401 [28], TS 23.060 [2], TS 23.501 [48] and TS 23.502 [49].
ESFB = Emergency Services Fallback for 5GS as defined in TS 23.501 [48] and TS 23.502 [49].
NOTE 1: If the UE selects the CS domain and initiates a normal call using the dialled local emergency number (see clause 7.1.2), and the UE enters limited service state (e.g. due to a Location Registration failing), then the UE camps on an acceptable cell (see TS 23.122 [41]) and may proceed with the EMC by initiating an emergency call in limited service state.
NOTE 2: Use of the same domain as for a non-EMC is restricted to UTRAN, E-UTRAN and NG-RAN access (e.g. excludes WLAN).
NOTE 3: This NOTE applies to a UE in dual registration mode as defined in TS 23.501 [48]. A dual registration mode UE that is registered to both EPC and 5GC assumes attachment, for the purpose of the "PS Attached" column, to whichever of EPC or 5GC indicates EMS as "Y". When both EPC and 5GC indicate EMS as "Y", the UE shall assume attachment to either EPC or 5GC based on implementation. A UE that is registered to both EPC and 5GC does not use emergency services fallback and ignores the ESFB condition when performing domain selection.
NOTE 4: The other 3GPP RAT for row C and row F can be any of UTRA, E-UTRAN connected to EPC, E-UTRA connected to 5GC or NR connected to 5GC that is supported by the UE and differs from the RAT to which the UE is currently attached in the PS domain (or is assumed to be attached based on NOTE 3).
NOTE 5: The condition 'ESFB is "Y"' only applies for a UE that is camped on or connected to 5GS via NR or via E-UTRA and that supports Emergency Services Fallback. In that case the emergency call will be provided over E-UTRAN or E-UTRA connected to 5GC as defined in procedures in TS 23.502 [49]. The condition 'ESFB is "Y"' is taken into consideration by the UE only when the network has indicated EMS = "N" for the RAT on which the UE is camping or connected.
NOTE 6: For 5GS, the value of the column "EMS" is for the RAT that UE is camped on or is connected to.
NOTE 7: As an implementation option, when the first attempt uses PS and fails for reasons other than related to IMS, the second attempt may use PS with a different 3GPP RAT. In this case the UE, can make a third attempt using CS.

H.6 eCall over IMS

This clause details the domain priority and selection (see clause 7.3) for a UE that attempts to make an eCall over IMS session using E-UTRAN or E-UTRA connected to 5GC radio access networks based on the availability of the CS or PS domains and the network support for IMS emergency, eCall over IMS and IMS voice over PS.

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

Table H.2: Domain Selection Rules for eCall over IMS session attempts for E-UTRAN or E-UTRA connected to 5GC radio access networks

	PS Available	VoIMS	EMS	ECL	First eCall Attempt	Second eCall Attempt
A	Y	Y	Y	Y	PS	CS if available
B	Y	Y	Y	N	CS if available	PS (UE establishes IMS emergency session)
C	Y	Y or N	N	N	CS if available	No attempt is made in the PS domain
D	Y	N	Y	Y	PS or CS if available	CS if first attempt in PS PS if first attempt in CS
E	Y	N	Y	N	CS if available	PS (UE establishes IMS emergency session)
F	N		-	-	CS if available	

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 23.502 [49] for E-UTRA connected to 5GC only.
EMS = IMS Emergency Services supported as indicated by Emergency Service Support indicator as defined in TS 23.401 [28] and TS 23.501 [48] and TS 23.502 [49] for E-UTRA connected to 5GC only.
ECL = eCall Over IMS support as indicated by the eCall support indicator defined in TS 23.401 [28] and TS 23.501 [48] for E-UTRA connected to 5GC only.

NOTE: For a UE camped on an E-UTRA cell connected to both 5GC and EPC, a UE assumes "PS Available" and "ECL" apply to whichever of 5GC or EPC are indicated as providing eCall over IMS support as defined in TS 23.501 [48]. When support by both is indicated, a UE may select either according to the UE implementation.

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 (normative): IMS emergency services using WLAN access to EPC

J.1 General

This annex includes additional clarifications when the IP-CAN corresponds to a WLAN access to EPC.

Both trusted WLAN access (S2a) and Untrusted WLAN access (S2b) to EPC for emergency sessions are supported.

NOTE: This annex only applies to EPC access using S2a or S2b.

The UE may issue an Emergency session over WLAN access to EPC only when 3GPP access for emergency call is not possible or available (e.g. no 3GPP coverage).

Further details on the procedures defined for WLAN access to EPC support of support emergency sessions are defined in TS 23.402 [29].

J.2 UE specific behaviour

Procedure for determining the list of emergency numbers:

- In addition to the emergency numbers and associated types stored either on the USIM or on the user equipment specified in TS 22.101 [8] clause 10.1.1, the UE shall use the stored Local Emergency Numbers List received from the 3GPP network to detect that the number dialled is an emergency number.

- If a UE has a SIM/USIM and has received a list of emergency numbers, and associated types via mobility management procedures as described in TS 24.301 [33] or TS 24.008 [13] when connected to the PLMN using GERAN, UTRAN, E-UTRAN or TS 24.501 [52] when connected to NG-RAN or non-3GPP access connected to 5GC , or, for a UE supporting access to 5GC using untrusted non-3GPP access, as specified in Annex L, the UE shall use this list to determine if the dialled digits correspond to an emergency call as long as the UE has determined that the list is valid (see clause 4.1).

- The UE may also determine that the dialled digits and associated types or URN information correspond to an emergency call based on the list of emergency numbers retrieved by one of the following means:

NOTE: How the UE uses two lists (a list of emergency numbers and associated types or URN information received via mobility management procedures and a list of emergency numbers and associated types or URN information retrieved via the WLAN) is a stage 3 decision.

  a) via Access Network Query Protocol (ANQP) procedures defined in IEEE Std 802.11 2012 [47] from the associated WLAN AP upon completing authentication with the trusted WLAN, with management frame protection enabled.

  b) via a previous query to a DNS only when that DNS is in the same country as the UE and is an internal DNS server in the 3GPP network whose address is acquired from the ePDG; or

  c) via IKEv2 procedures from ePDG.

- The list of downloaded emergency numbers shall be deleted at country change or, if the particular list is only valid for a PLMN -see TS 22.101 [8] clause 10.4.1), at successfull registration with a different PLMN.

For the specific case where the UE has selected to make an emergency call over WLAN access to EPC (hence the UE has detected that the target URI or dialled digits correspond to an emergency sessions), the UE shall use the following procedures:

- The UE shall establish an emergency PDN connection over WLAN and shall perform an IMS emergency registration before sending an IMS emergency session request.

- The UE shall include any available location information in the IMS emergency session request. This is further detailed in TS 23.228 [1].
- For the media supported during IMS emergency sessions, media codec and format support is specified in TS 26.114 [34].
- For the support of DRVCC on emergency call on WLAN, see TS 23.237 [32].

A UE shall not establish an emergency PDN connection over WLAN if the UE initiated a normal (i.e. non-emergency) session and is subsequently informed by the network that the ongoing session is accepted by the network even though it is an emergency session.

J.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 EPC access over WLAN is used:

- the IP-CAN bearer resource is a PDN connection dedicated for emergency services. The TS 23.402 [29] describes how to indicate that a PDN connection request is for emergency;
- For registration requests received from an emergency PDN connection, the P-CSCF shall reject any IMS registration which is not for the emergency purpose.

NOTE 1: When the IMS network detects that the UE is establishing an emergency session over WLAN access to EPC while the UE is not in its Home country, local policies in the Home IMS network may determine whether to nevertheless handle the emergency session

For the high level procedures (as described in clause 7.1.2) the following statements apply for Non UE detectable emergency calls when WLAN access to EPC is used:

- The P-CSCF may reject the session initiation request with an indication that this is an emergency session or may allows the session initiation request to continue.

The following flow contains a high level description of the emergency service procedures performed over WLAN access to EPC when the UE can detect that an emergency PDN connection is being needed. This flow provides details (or references) related with WLAN access to EPC on top of the general procedure described in clause 7.1.

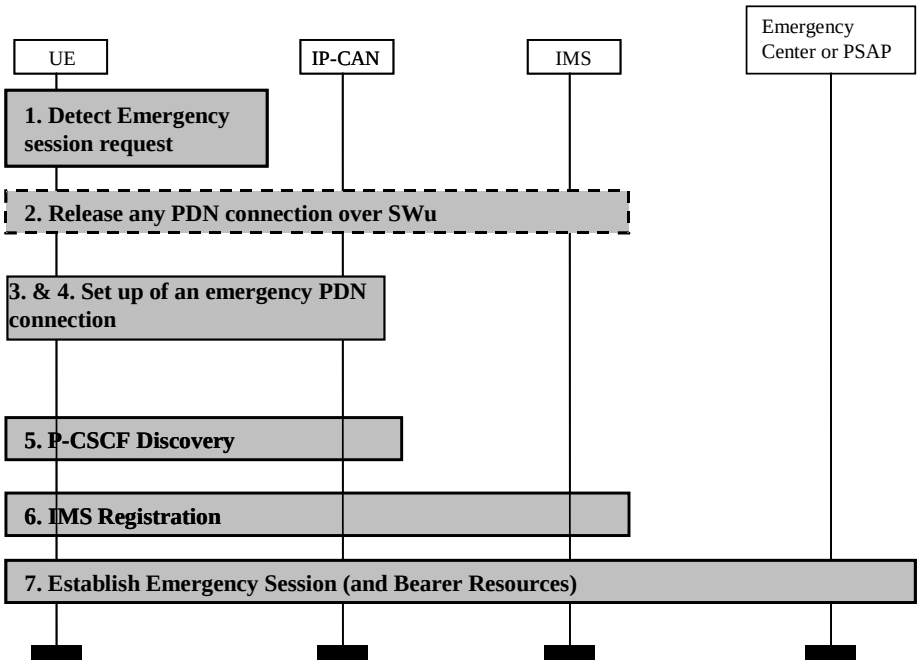


Figure J.3: Terminal Detected Emergency Calls (Un trusted WLAN access to EPC)

The following steps are performed:

1. Same as step 1 of Figure 7.1
2. The UE releases any PDN connection it may have over untrusted access to EPC.
3. Void.
4. As described in TS 23.402 [29], the UE selects an ePDG for emergency services and sets-up a PDN connection for emergency services. The UE is assigned an IP address at this stage.

NOTE 2: No specific WLAN AP selection is carried out to support emergency services.

5. Same as step 5 of Figure 7.1.
6. Same as step 6 of Figure 7.1.
7. Same as step 7 of Figure 7.1.

J.4 Location handling

When a UE performs an emergency registration or initiates an emergency session over WLAN access to EPC the UE provides location information that is further defined in TS 23.228 [1].

If the operator policy requires network provided location using PCC-based solutions for the UE location, the P-CSCF may retrieve location information from the access network as defined in TS 23.203 [20] and includes it in the emergency session request, as described in TS 23.228 [1].

Annex K (normative): Support of IMS emergency sessions for roaming users in deployments without IMS-level roaming interfaces

K.1 General

This annex includes network impact and call flows for support of IMS emergency sessions for roaming users in deployments without IMS-level roaming interface between the P-CSCF in the VPLMN and the S-CSCF in the HPLMNs. This annex is only applicable to UTRAN and E-UTRAN access networks.

IMS authentication is performed by linking the IMS registration to user's EPS authentication based on the user's IP address and IMSI. This mechanism is similar to GIBA (GPRS-IMS bundled authentication) specified in TS 33.203 [44]. The P-CSCF performs the GIBA procedure over Gm with the UE as defined in TS 24.229 [19]. If this procedure is not supported, UE may peform anonymous emergency session. A callback number for the user may also be retrieved via the PCRF.

K.2 Functional description

K.2.1 General

This clause lists the additional functionality in the network that is required to support IMS emergency sessions for roaming users in network deployments where there are no IMS-level roaming interfaces between the serving IMS network and the home IMS network.

K.2.2 P-CSCF

In addition to the functionality described in clause 6.2.1, the P-CSCF supports the functionality listed below:

- P-CSCF shall be able to retrieve the UE/user's IMSI, IMEI and MSISDN (if available) from the PCRF.
- P-CSCF may support the GIBA procedure over Gm as defined in TS 24.229 [19].
- P-CSCF may verify the IMSI/IMEI provided in the SIP REGISTER message against the IMSI/IMEI provided by the PCRF.

K.2.3 PCRF

- PCRF shall be able to provide the IMSI, the ME Identity (IMEISV), and MSISDN (if available) over Rx to the P-CSCF.

K.2.4 PGW

- PGW shall be able to prevent "source IP address spoofing" for IMS emergency PDN connections in case GIBA authentication defined in TS 33.203 [44] is used as part of emergency IMS registration.

K.2.4 HSS

- The EPS user subscription should contain exactly one MSISDN which should be the same as that in the IMS profile.

K.3 IMS Emergency Registration and Session Establishment

The call flow for support of IMS emergency sessions for roaming users in deployments without IMS-level roaming interfaces for UTRAN and E-UTRAN access networks is described in Figure K.3-1.

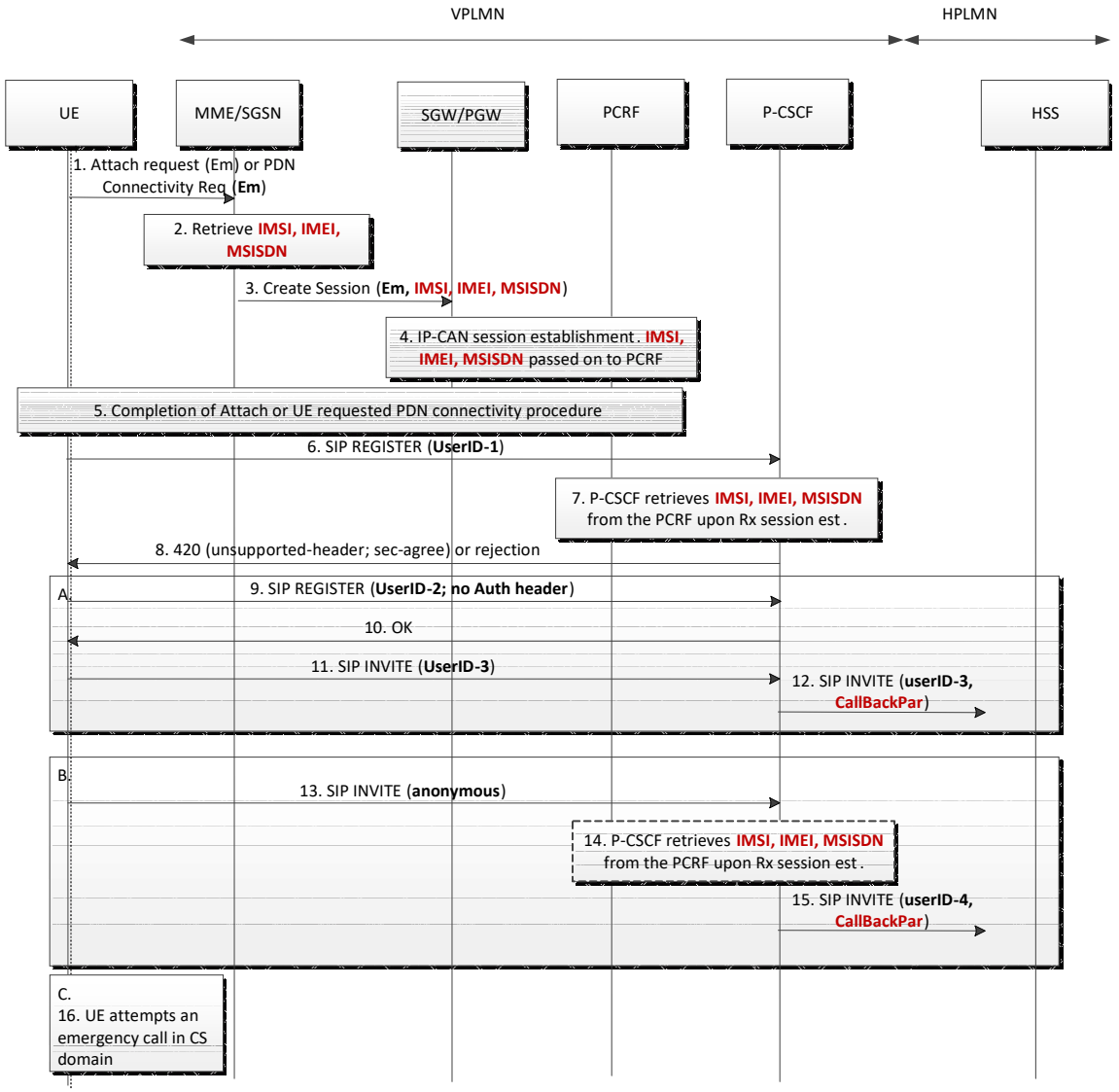


Figure K.3-1: IMS Emergency Session Establishment in deployments without IMS roaming interface between VPLMN and HPLMN

1. UE establishes a PDN connection for IMS emergency services.
2. IMSI and IMEI(SV) are retrieved from the UE. The MSISDN (if available) is provided by the HSS.
3. MME/SGSN sends a Create Session Request towards the PGW including the IMSI, the IMEI(SV) and the MSISDN (if available) as specified in TS 23.401 [28].
4. PGW establishes an IP-CAN session with the PCRF as described in TS 23.401 [28] and TS 23.203 [20]. The IP-CAN session is identified with UE's IPv4 address of IPv6 prefix associated with the PDN connection for IMS emergency services. The IMSI, the IMEI(SV) and the MSISDN (if available) are passed to the PCRF as part of the IP-CAN session establishment.
5. UE completes the Attach or UE requested PDN connection procedure.

Steps 6-12 apply in case the UE performs IMS Emergency Registration, based on conditions specified in clause 4.1 e.g. UE is aware that it has sufficient IMS authentication material.

6. UE initiates IMS emergency registration by sending a SIP REGISTER (UserID-1) message. The UserID-1 parameter is an IMPI and optionally an IMPU.

7a. Upon reception of the SIP REGISTER message the P-CSCF determines that there is no IMS NNI to the user's HPLMN. The P-CSCF requests the PCRF for EPS-level identities (e.g. IMSI, IMEI(SV), MSISDN) in the Rx session establishment request.

7b. The PCRF performs session binding based on the UE's IP address/prefix (as defined in TS 23.203 [20] clause 6.1.1.2) and provides one or more EPS-level identities and the MSISDN (if available) to the P-CSCF.

8. Based on operator configuration and if the network supports the GIBA procedure over Gm as defined in TS 24.229 [19], the P-CSCF responds with a 420 response with sec-agree value listed in the unsupported header field. Otherwise it rejects the IMS registration request with SIP 403 (Forbidden) as defined in TS 24.229 [19]. If the network supports anonymous IMS emergency sessions, P-CSCF may add an indication whether it supports anonymous IMS emergency sessions to the 403 or 420 response.

Steps 9-12 apply in case the P-CSCF has responded with a 420 response in step 8 and if the UE supports GIBA procedure as part of emergency IMS registration (irrespective of whether indication of anonymous IMS emergency session support was included in step 8).

9. UE according to TS 24.229 [19], performs a new initial registration by sending a SIP REGISTER (UserID-2, IMEI) message and without inclusion of the Authorization header field. UserID-2 is an a public user identity derived from IMSI. P-CSCF may verify the IMSI/IMEI provided by the PCRF in step 7b against the IMSI/IMEI derived from the public user identity provided by the UE, prior to accepting the SIP REGISTER message.

10. P-CSCF accepts the registration with 200 OK and provides a tel-URI based on the MSISDN (if available) received from PCRF in step 7b to the UE. From the UE point of view, the procedure is the same as specified for GIBA (GPRS-IMS bundled authentication) procedures in TS 24.229 [19].

11. UE then attempts an IMS emergency session by sending a SIP INVITE (UserID-3) message. UserID-3 is set to UE's public identity (i.e. MSISDN as Tel-URI received in step 10).

12. The P-CSCF verifies whether the UserID-3 indicated in the SIP INVITE message complies with the tel-URI that was provided to the UE. If compliant, P-CSCF forwards the SIP INVITE towards the PSAP including a callback parameter (CallBackPar) in the form of TEL-URI derived from the MSISDN received in step 7. The procedure stops here.

Steps 13-15 apply if the UE attempts anonymous IMS emergency session, e.g. the P-CSCF has responded in step 8 with a 403 (Forbidden) response, or the P-CSCF has responded in step 8 with 420 response and the UE does not support GIBA as part of emergency IMS registration, or if the UE skipped IMS emergency registration:

13. The UE may attempt an unauthenticated IMS emergency session including an "anonymous user" parameter in the SIP INVITE message.

14. Upon reception of the SIP INVITE the P-CSCF either internally retrieves the one or more EPS-level identities and the MSISDN (if available) that were received in step 7b, or performs step 7 again.

15. The P-CSCF forwards the SIP INVITE (UserID-4, CallBackPar) towards the PSAP. UserID-4 is derived from one of the EPS-level identities received in step 7b. CallBackPar in the form of TEL-URI is derived from the MSISDN received in step 7b. The procedure stops here.

Step 16 applies if the UE attempts an emergency call in the CS domain as specified in clause 4.1:

16. Subsequent to the IMS registration failure in step 8 or subsequent to an anonymous SIP INVITE attempt the UE may attempt an emergency call in the CS domain.

K.4 Non UE detectable Emergency Session

In addition to clause 7.1.2, the following is applicable for this scenario:

- It is recommended that local emergency call numbers are provided to the UE according to the procedures specified in TS 24.501 [52], TS 24.301 [33], TS 24.008 [13] or Annex J.2. This helps to reduce the number of non-UE detected emergency numbers even for those PLMNs where only a subset of the local emergency numbers can be downloaded to the UEs.

- When the UE registers in the IMS, the P-CSCF may retrieve the VPLMN-ID of the UE as described in TS 23.228 [1], clause W.3 and may access a database to obtain a list of all local emergency numbers for the visited PLMN, if not already available in the P-CSCF. These numbers are used for detection of non UE detectable emergency calls during IMS session setup. The database of PLMN- specific emergency numbers and its interface with the P-CSCF are not specified by 3GPP.

Annex L (normative): IMS emergency services using untrusted non-3GPP access to 5GC

L.1 General

This annex includes additional clarifications when the IP-CAN corresponds to a untrusted non-3GPP access to 5GC.

In this release of the specification, only untrusted non-3GPP access to 5GC for emergency sessions are supported.

The UE may issue an Emergency session over untrusted non-3GPP access to 5GC only when 3GPP access for emergency call is not possible or available (e.g. no 3GPP coverage).

Further details on the procedures defined for untrusted non-3GPP access to 5GC support of support emergency sessions are defined in TS 23.502 [49].

L.2 UE specific behaviour

Procedure for determining the list of emergency numbers:

- In addition to the emergency numbers and associated types stored either on the USIM or on the user equipment specified in TS 22.101 [8] clause 10.1.1, the UE shall use the stored Local Emergency Numbers List received from the 3GPP network to detect that the number dialled is an emergency number.

- If a UE has a SIM/USIM and has received a list of emergency numbers and associated types or URN information via mobility management procedures as described in TS 24.301 [33] and TS 24.008 [13] when connected to the PLMN using GERAN, UTRAN, E-UTRAN, or TS 24.501 [52] when connected to NG-RAN or non-3GPP access connected to 5GC, or, for a UE supporting access to EPC via WLAN, as specified in Annex J, the UE shall use this list to determine if the dialled digits correspond to an emergency call as long as the UE has determined that the list is valid (see clause 4.1).

NOTE: How the UE uses two lists (a list of emergency numbers and associated types or URN information received via mobility management procedures and , for a UE supporting access to EPC via WLAN, a list as specified in Annex J) is a stage 3 decision.

- The list of downloaded emergency numbers shall be deleted at country change or, if the particular list is only valid for a PLMN (see TS 22.101 [8] clause 10.4.1), at successfull registration with a different PLMN.

For the specific case where the UE has selected to make an emergency call over untrusted non-3GPP access to 5GC (hence the UE has detected that the target URI or dialled digits correspond to an emergency sessions), the UE shall use the following procedures:

- The UE shall establish an emergency PDU session over untrusted non-3GPP and shall perform an IMS emergency registration before sending an IMS emergency session request.

- The UE shall include any available location information in the IMS emergency session request. This is further detailed in TS 23.228 [1].

- For the media supported during IMS emergency sessions, media codec and format support is specified in TS 26.114 [34].

A UE shall not establish an emergency PDU session over untrusted non-3GPP access if the UE initiated a normal (i.e. non-emergency) session and is subsequently informed by the network that the ongoing session is accepted by the network even though it is an emergency session.

L.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 5GC access over untrusted non-3GPP access is used:

- the IP-CAN bearer resource is a PDU session dedicated for emergency services. TS 23.502 [49] describes how to indicate that a PDU Session Request is for emergency.

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

NOTE 1: When the IMS network detects that the UE is establishing an emergency session over untrusted non-3GPP access to 5GC while the UE is not in its Home country, local policies in the Home IMS network may determine whether to nevertheless handle the emergency session.

For the high-level procedures (as described in clause 7.1.2) the following statements apply for Non UE detectable emergency calls when untrusted non-3GPP access to 5GC is used:

- The P-CSCF may reject the session initiation request with an indication that this is an emergency session or may allows the session initiation request to continue.

The following flow contains a high-level description of the emergency service procedures performed over untrusted non-3GPP access to 5GC when the UE can detect that an emergency PDU session is being needed. This flow provides details (or references) related with untrusted non-3GPP access to 5GC on top of the general procedure described in clause 7.1.

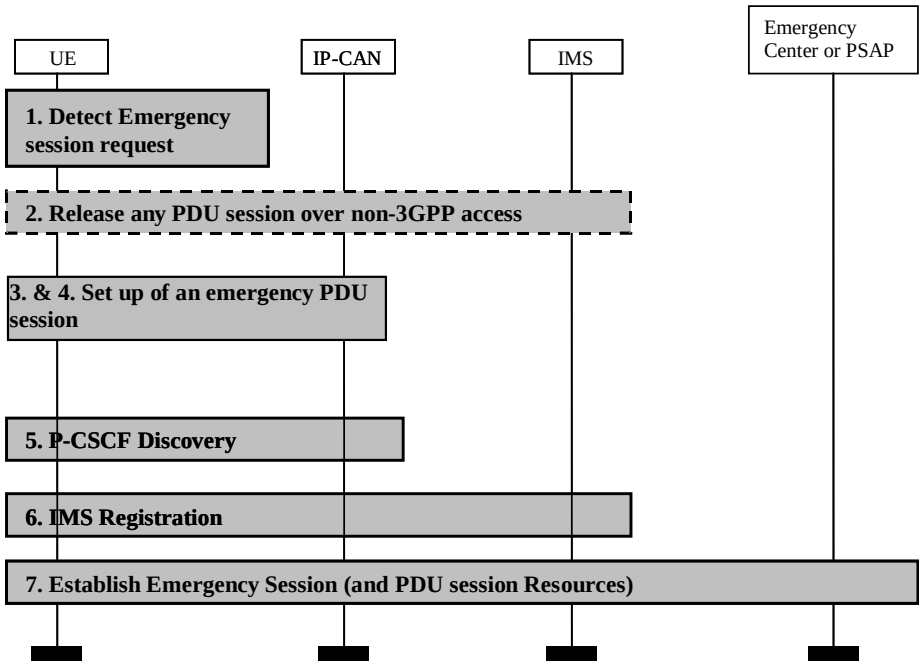


Figure L.3: Terminal Detected Emergency Calls (non-3GPP untrusted access to 5GC)

The following steps (numbering being the same as in figure 7.1) are performed:

1. Same as step 1 of Figure 7.1.

2. In some exceptional cases (e.g. in congestion situation), Tthe UE may release some PDU session it may have over untrusted non-3GPP access to 5GC.

3. Void (no "bearer registration" as described in step 3 of Figure 7.1).

4. As described in TS 23.502 [49], the UE selects an N3IWF as for accessing regular services and sets-up a PDU session for emergency services. The UE is assigned an IP address at this stage.

NOTE 2: When untrusted non-3GPP access is WLAN, no specific WLAN AP selection is carried out to support emergency services.

5. Same as step 5 of Figure 7.1.

6. Same as step 6 of Figure 7.1.

7. Same as step 7 of Figure 7.1, except that eCall is not supported via untrusted non-3GPP access.

L.4 Location handling

When a UE performs an emergency registration or initiates an IMS emergency session over untrusted non-3GPP access to EPC the UE provides location information that is further defined in TS 23.228 [1].

For untrusted non-3GPP access to 5GC, provided location information can only correspond to the UE IP address seen by the N3IWF and used for traffic destined towards the UE.

Annex M (informative): Change history

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
2010-12	SA#50	SP-100694	0182	3	B	Retrieval of reference location for emergency session routed via the S-CSCF	11.0.0
2011-01	-	-	-	-	-	Update of LTE logo to LTE-Advanced logo	11.0.1
2011-03	SA#51	SP-110063	0186	1	A	PSAP call back handling in S-CSCF	11.1.0
2011-09	SA#53	SP-110455	0189	1	A	Correction of emergency procedures	11.2.0
2011-09	SA#53	SP-110469	0190	1	C	Emergency location information for fixed broadband access	11.2.0
2011-12	SA#54	SP-110740	0192	1	F	Media support during an IMS emergency session	11.3.0
2011-12	SA#54	SP-110730	0197	1	A	Correction of Emergency procedures	11.3.0
2011-12	SA#54	SP-110737	0201	1	A	Clarification on S-CSCF handling when receiving emergency session from AS.	11.3.0
2011-12	SA#54	SP-110869	0204	5	A	Clarifications on non UE detectable emergency call	11.3.0
2011-12	SA#54	SP-110740	0205	2	B	Media support on PSAP callback	11.3.0
2012-03	SA#55	SP-120080	0207	1	B	Codecs supported for IMS emergency sessions	11.4.0
2012-03	SA#55	SP-120081	0208	1	B	Support of Network-provided Location for IMS functionality	11.4.0
2012-03	SA#55	SP-120080	0212	3	B	Domain Selection Rules for IMSESOM with E-UTRAN and UTRAN Access	11.4.0
2012-06	SA#56	SP-120250	0215	1	F	Handling of Emergency Registrations at Home IMS	11.5.0
2012-06	SA#56	SP-120250	0216	1	F	S-CSCF and AS in Emergency Calls	11.5.0
2012-12	SA#58	SP-120250	0220	1	A	Defining S-CSCF procedures for registration and emergency registration relationships	11.6.0
2013-06	SA#60	SP-130309	0223	1	F	Domain selection before UE detectable emergency session	11.7.0
2013-06	SA#60	SP-130309	0226	2	F	Domain selection in the event emergency bearer services are not supported	11.7.0
2013-09	SA#61	SP-130367	0232	2	A	Requirement Alignment for emergency registration and call back	11.8.0
2013-09	SA#61	SP-130376	0234	1	C	Requirement Alignment for call back	11.8.0
2013-12	SA#62	SP-130518	0251	1	A	Treatment of a 380 Response for an undetected IMS Emergency Call	11.9.0
2014-03	SA#63	SP-140097	0259	1	A	Non UE detected emergency call correction when the retry attempt is made in CS domain	11.10.0
2014-03	SA#63	SP-140098	0261	-	A	Clarification when using a private network for emergency calls	11.10.0
2014-06	SA#64	SP-140247	0264	3	A	380 - Emergency call clarification	11.11.0
2014-09	SA#65	-	-	-	-	Update to Rel-12 version (MCC)	**12.0.0**
2015-03	SA#67	SP-150109	0275	1	F	Correction to support of I-WLAN in TS 23.167	12.1.0
2015-09	SA#69	SP-150503	0279	2	B	Location to Support Emergency services over WLAN access to EPC	**13.0.0**
2015-09	SA#69	SP-150503	0280	2	B	Introduction of the Support of Emergency services over WLAN access to EPC	**13.0.0**
2015-12	SA#70	SP-150614	0281	-	F	Clarification on the UE behavoir when initiates the emergency call	13.1.0
2016-03	SA#71	SP-160162	0283	-	F	Correction of 3GPP2 specification reference	13.2.0
2016-06	SA#72	SP-160299	0284	9	B	eCall over IMS - Initial MSD	**14.0.0**
2016-06	SA#72	SP-160299	0286	5	B	Domain Selection for eCall Over IMS	**14.0.0**
2016-06	SA#72	SP-160299	0287	2	B	Transfer of Updated MSD for eCall Over IMS	**14.0.0**
2016-06	SA#72	SP-160302	0289	2	B	Support for Sh in LRF for NPLI, and Support for UE updated Location mid-emergency session over emergency signalling channel	**14.0.0**
2016-06	SA#72	SP-160302	0292	3	B	WLAN to CS session continuity for Emergency call over WLAN	**14.0.0**
2016-06	SA#72	SP-160302	0294	3	B	Determine of Emergency number for call over WLAN	**14.0.0**
2016-06	SA#72	SP-160304	0295	3	C	Support of IMS emergency sessions for roaming users in deployments without IMS-level roaming interfaces	**14.0.0**
2016-09	SA#73	SP-160659	0282	4	B	Providing subscriber ID in case of anonymous emergency calls	14.1.0
2016-09	SA#73	SP-160652	0296	2	B	Support for dispatchable civic location for indoor environments for North American.	14.1.0
2016-09	SA#73	SP-160647	0297	1	F	Editorial change to Transfer of Updated MSD for eCall Over IMS call flow	14.1.0
2016-09	SA#73	SP-160658	0299	1	B	Indication for support of anonymous IMS emergency sessions	14.1.0
2016-09	SA#73	SP-160651	0300	3	C	Capturing solution for non UE detectable emergency call for S8 Home routing	14.1.0
2016-09	SA#73	SP-160647	0301	2	F	Clarifications when inband is used by a UE to convey MSD	14.1.0
2016-09	SA#73	SP-160647	0302	-	F	Definition for eCall Over IMS	14.1.0
2016-09	SA#73	SP-160654	0303	2	B	Allowing ICS MSC to interact with IMS for IMS emergency call handling.	14.1.0
2016-12	SA#74	SP-160817	0305	3	F	Update with SEW2 capabilities	14.2.0
2016-12	SA#74	SP-160816	0306	1	F	Correction from IMPI to IMPU	14.2.0

2016-12	SA#74	SP-160817	0311	3	F	Correction to emergency number determination for call over WLAN	14.2.0
2016-12	SA#74	SP-160817	0312	-	F	Enable use of SUPL to locate a UE with WLAN Access	14.2.0
2016-12	SA#74	SP-160817	0313	2	F	Unsolicited Provision of UPLI by a UE for WLAN Access	14.2.0
2017-03	SA#75	SP-170053	0314	2	F	Clarification of functionality for interconnection of emergency call over II-NNI	14.3.0
2017-03	SA#75	SP-170079	0315	1	F	Alignment of emergency procedures	14.3.0
2017-06	SA#76	SP-170367	0316	1	F	Downloading emerg number from ePDG	14.4.0
2017-09	SA#77	SP-170723	0318	-	F	Clarification for voice domain selection rules applicability in Annex H	14.5.0
2017-12	SA#78	SP-170919	0319	2	B	Support of IMS Emergency Calls for NG-RAN access to 5GS	**15.0.0**
2018-03	SA#79	SP-180094	0320	3	F	Emergency services over 5GC via untrusted non-3GPP access	15.1.0
2018-03	SA#79	SP-180094	0321	2	F	Handling of emergency sessions over untrusted N3GPP access in 5GS	15.1.0
2018-03	SA#79	SP-180094	0324	1	F	Delivery of local emergency numbers in NAS	15.1.0
2018-03	SA#79	SP-180094	0325	2	F	Addition of Emergency Services Support using Fallback to Domain Selection Rules	15.1.0
2018-06	SA#80	SP-180479	0326	1	F	Clarification on Domain Selection for Emergency Service.	15.2.0
2018-06	SA#80	SP-180475	0327	1	F	Domain selection for eCall over IMS	15.2.0
2018-06	SA#80	SP-180475	0329	-	F	Correction on domain selection for eCall over IMS	15.2.0
2018-06	SA#80	SP-180475	0330	2	F	Correction to NOTE 5 in domain selection for Emergency services	15.2.0
2018-09	SA#81	SP-180712	0331	2	F	Update on Domain Selection Rules for emergency session attempts	15.3.0
2018-09	SA#81	SP-180712	0332	-	F	UE handling of emergency numbers list when using untrusted non-3GPP access to 5GC	15.3.0
2018-09	SA#81	SP-180711	0334	-	A	Correct conditions for using valid local emergency number list	15.3.0
2018-09	SA#81	SP-180712	0335	-	F	Domain selection for dual registration mode UE	15.3.0
2018-09	SA#81	SP-180712	0336	2	F	Support of eCall and emergency call when eUTRAN is connected to 5GS and EPS	15.3.0
2018-12	SA#82	SP-181083	0337	1	F	Correct procedures for obtaining local emergency number list	15.4.0
2018-12	SA#82	SP-181083	0338	1	F	Correct validity of local emergency number list	15.4.0
2018-12	SA#82	SP-181083	0339	1	F	Correcting usage of emergency service indication and emergency session indication	15.4.0
2018-12	SA#82	SP-181083	0341	-	C	More Flexible Domain selection for Emergency Calls using the PS Domain	15.4.0