**3GPP TSG-SA WG2 Meeting #143-e (e-meeting) *S2-210xxxx***

**24 February- 9 March 2021, Elbonia *(revision of S2-200xxxx)***

|  |
| --- |
| *CR-Form-v12.0* |
| **CHANGE REQUEST** |
|  |
|  | **23.167** | **CR** | **xxxx** | **rev** | **-** | **Current version:** | **16.3.0** |  |
|  |
| *For* [***HE******LP***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)*on using this form: comprehensive instructions can be found at* [*http://www.3gpp.org/Change-Requests*](http://www.3gpp.org/Change-Requests)*.* |
|  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME | **X** | Radio Access Network | **X** | Core Network | **X** |

|  |
| --- |
|  |
| ***Title:***  | Support for IMS emergency over SNPN |
|  |  |
| ***Source to WG:*** | Qualcomm Incorprorated |
| ***Source to TSG:*** | SA2 |
|  |  |
| ***Work item code:*** | eNPN |  | ***Date:*** | 2021-02-24 |
|  |  |  |  |  |
| ***Category:*** | **C** |  | ***Release:*** | Rel-17 |
|  | *Use one of the following categories:****F*** *(correction)****A*** *(mirror corresponding to a change in an earlier release)****B*** *(addition of feature),* ***C*** *(functional modification of feature)****D*** *(editorial modification)*Detailed explanations of the above categories canbe found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | *Use one of the following releases:Rel-8 (Release 8)Rel-9 (Release 9)Rel-10 (Release 10)Rel-11 (Release 11)Rel-12 (Release 12)**Rel-13 (Release 13)Rel-14 (Release 14)Rel-15 (Release 15)Rel-16 (Release 16)* |
|  |  |
| ***Reason for change:*** | This CR is introducing changes in TS 23.167 for support of Emergency Services for SNPNs based on the conclusions of Key Issue #3 in TR 23.700-07. |
|  |  |
| ***Summary of change:*** | * Signalling of emergency call numbers from SNPN
* Support for non-detectable emergency calls from SNPN
* Support for emergency session from SNPN
* Domain selection for emergency session from SNPN
* IMS emergency services using SNPN access via PLMN
 |
|  |  |
| ***Consequences if not approved:*** | No support for emergency services from SNPN |
|  |  |
| ***Clauses affected:*** | 4.1, 7.1.2, 7.2, H.1, H.2, H.5, K.3, K.4, L.1, L.3, L.4 |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** |  | **X** |  Other core specifications  | TS/TR ... CR ...  |
| ***affected:*** |  | **X** |  Test specifications | TS/TR ... CR ...  |
| ***(show related CRs)*** |  | **X** |  O&M Specifications | TS/TR ... CR ...  |
|  |  |
| ***Other comments:*** |  |
|  |  |
| ***This CR's revision history:*** |  |

\*\*\*\* First Change \*\*\*\*

## 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 non-3GPP access to 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 or SNPN). 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 if 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.

\*\*\*\* Next Change \*\*\*\*

### 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 or a P‑CSCF in the SNPN 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 or the P-CSCF of the SNPN 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 or visited SNPN forwards that request to an Emergency CSCF in the same network. The P-CSCF in the home PLMN or visited SNPN 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.

\*\*\*\* Next Change \*\*\*\*

## 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 or visited SNPN 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 or visited SNPN).

- 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 or visited SNPN 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.

\*\*\*\* Next Change \*\*\*\*

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].

If an SNPN supports other emergency numbers than those listed in TS 22.101 [8], the UE is directly connected to the SNPN using NR 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 24.501 [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 supported with E-UTRAN and NG-RAN. 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].

\*\*\*\* Next Change \*\*\*\*

# 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 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.

- If the broadcast indicator in an NR cell indicates that the cell provides access to SNPNs and that 5GC supports emergency services, the UE shall only register to the core network of the SNPN that indicates support for emergency services. If broadcast indicators indicate that one or more SNPNs and/or PLMNs support emergency services then the UE initiates emergency services to either SNPN or PLMN according to UE implementation.

\*\*\*\* Next Change \*\*\*\*

# 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 CSCS 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 CSCS 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 CSCS 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 PSPS 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.NOTE 8: For SNPN, as defined in TS 23.501 [48] the only RAT supported is NR and there is no support for Emergency Services Fallback. |

\*\*\*\* Next Change \*\*\*\*

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 or VSNPN and the S-CSCF in the HPLMNs or Home SP domain in case the visited network is SNPN. This annex is only applicable to UTRAN, E-UTRAN and NG-RAN access networks.

IMS authentication is performed by linking the IMS registration to user's EPS or 5GS 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 perform anonymous emergency session. A callback number for the user may also be retrieved via the PCRF or PCF.

\*\*\*\* Next Change \*\*\*\*

# 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, E-UTRAN or NG-RAN 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 or VSNPN and HPLMN or Home SP

1. UE establishes a PDN connection (for EPC) or PDU session (for 5GC) for IMS emergency services.

2. For EPC, IMSI and IMEI(SV) are retrieved from the UE. The MSISDN (if available) is provided by the HSS.

 For 5GC, the SUPI and PEI are retrieved from the UE context stored in the AMF; the SUPI needs to contain an IMSI and the PEI needs to contain an IMEI(SV). The GPSI (if available) is provided by the UDM; the GPSI needs to contain an MSISDN.

3. For EPC: 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].

 For 5GS: AMF sends a Nsmf\_PDUSession\_CreateSMContextRequest towards the SMF/UPF including the SUPI, the PEI and the GPSI (if available) as specified in TS 23.502 [49].

4. For EPC, 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.

 For 5GC, SMF establishes an SM Policy Association with the PCF as described in TS 23.502 [49] and TS 23.503 [51]. The PDU session is identified with UE's IPv4 address or IPv6 prefix. The SUPI, PEI, GPSI (if available) and emergency DNN are passed to the PCF.

5. The Attach or UE requested PDN connection procedure (for EPC) or the PDU Session Establishment procedure (for 5GC) is being completed.

Steps 6-12 apply if 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 or PCF for EPS-level identities (e.g. IMSI, IMEI(SV), MSISDN) in the Rx session establishment request. For 5GC, P-CSCF may use the Npcf\_PolicyAuthorization service as described in TS 23.502 [49] and TS 23.503 [51] instead of the Rx interface.

7b. For EPC, 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.

 For 5GC, the PCF performs session binding based on the UE's IP address/prefix (as defined in TS 23.503 [51]). If the Rx interface is used, the PCF extracts IMSI, IMEI(SV), and if available MSISDN from SUPI, PEI, and GPSI, respectively and provides the former identities to the P-CSCF. If the Npcf\_PolicyAuthorization service is used, the PCF provides SUPI, PEI, and if available GPSI, and the P-CSCF extracts IMSI, IMEI(SV), and if available MSISDN from those identities.

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 if 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 or PCF 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.

\*\*\*\* Next Change \*\*\*\*

# 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 or VSNPN 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/SNPN- specific emergency numbers and its interface with the P-CSCF are not specified by 3GPP.

Annex L (normative):
IMS emergency services using non-3GPP access to 5GC or SNPN access via PLMN

# L.1 General

This annex includes additional clarifications when the IP-CAN corresponds to a non-3GPP access to 5GC or when 3GPP IP-CAN of a PLMN is used to provide access to SNPN via N3IWF as defined in TS 23.501 [48].

Trusted and untrusted non-3GPP access to 5GC for emergency sessions are supported.

The UE may issue an Emergency session to 5GC of an SNPN via N3IWF and the 3GPP IP-CAN of a PLMN only when emergency calls are not supported or available using PLMN or SNPN 3GPP access directly.

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

Further details on the procedures defined for non-3GPP access to 5GC and access to SNPN 5GC over a PLMN to support emergency sessions are defined in TS 23.502 [49].

\*\*\*\* Next Change \*\*\*\*

# 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 non-3GPP access is used or when 3GPP IP-CAN of a PLMN is used to provide access to SNPN via N3IWF as defined in TS 23.501 [48]:

- 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 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 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 allow the session initiation request to continue.

The following flow contains a high-level description of the emergency service procedures performed over 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 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 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), the UE may release some PDU session it may have over non-3GPP access to 5GC or PLMN access to SNPN over via N3IWF.

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

4. As described in TS 23.502 [49]:

- in the case of untrusted access, the UE selects an N3IWF as for accessing regular services and sets-up a PDU session for emergency services;

- in the case of trusted access, the UE sets-up a PDU session for emergency services.

 The UE is assigned an IP address at this stage.

* in the case of access to SNPN via PLMN as defined in TS 23.501 [48] UE selects an N3IWF as for accessing regular services and sets up a PDU session for emergency services;

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

NOTE 3: When access to SNPN via PLMN is used, PLMN selection procedure is carried out as defined in TS 23.122 [41].

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.

\*\*\*\* Next Change \*\*\*\*

# 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 or access to SNPN via PLMN, provided location information can only correspond to the UE IP address seen by the N3IWF and used for traffic destined towards the UE.

\*\*\* End of Changes \*\*\*\*