**3GPP TSG-SA WG2 Meeting #143E S2-210XXXX**

**24 Feb - 03 March 2021, Electronic (revision of S2-210XXX)**

|  |
| --- |
| *CR-Form-v12.0* |
| **CHANGE REQUEST** |
|  |
|  | **23.167** | **CR** | **\_** | **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 |  | Radio Access Network |  | Core Network | **X** |

|  |
| --- |
|  |
| ***Title:***  | Support for Caller Identity Attestation and Assertion of Emergency sessions.  |
|  |  |
| ***Source to WG:*** | Ericsson |
| ***Source to TSG:*** | SA2 |
|  |  |
| ***Work item code:*** | TEI17\_SAPES |  | ***Date:*** | 2020-12-04 |
|  |  |  |  |  |
| ***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-15 (Release 15)Rel-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)* |
| ***`*** |  |
| ***Reason for change:*** | Identity assertion for IMS sessions is already supported based on the STIR/SHAKEN framework according to the requirements in TS 22.173 [53]. There are additional regulatory requirements to apply STIR/SHAKEN to priority calls and emergency calls, including callback from PSAP. |
|  |  |
| ***Summary of change:*** | In the case of emergency calls, it is proposed that the P-CSCF performs attestation for the calling identity.In addition, emergency calls may also be subject to Resource-Priority information signing as defined in RFC 8443. In this case, the attestation is applied to the Resource-Priority information by the IMS entity responsible for authorizing and handling the IMS session. This enables the inclusion of cryptographically signed assertions for the values populated in the Session Initiation Protocol (SIP) “Resource-Priority” header field, which is used for prioritization of communications resources. When an emergency session is delivered to an emergency network outside the domain of the operator, the IBCF should be capable of interacting with an Application Server (AS) that supports calling number and/or Resource-Priority information authentication/signing, and may do so based on configured operator policy, once it determines that an emergency call is destined for a Next Generation Emergency Services Network. By the same token the IBCF should be able to invoke an AS for verification of signed Resource-Priority information if available in the incoming request. |
|  |  |
| ***Consequences if not approved:*** | Not complying to regulatory requirements for emergency calls |
|  |  |
| ***Clauses affected:*** | 4.1, 6.2.12, 7.3, 7.4, K.2.2 |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** | **x** |  |  Other core specifications  | TS/TR .23.228.. CR ..XXXX.  |
| ***affected:*** |  | **X** |  Test specifications | TS/TR ... CR ...  |
| ***(show related CRs)*** |  | **X** |  O&M Specifications | TS/TR ... CR ...  |
|  |  |
| ***Other comments:*** |  |
|  |  |
| ***This CR's revision history:*** |  |

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of changes \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

## 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). 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.

29. An originating network that is processing an emergency session shall, if configured through operator policies, invoke an AS for the signing of attestation and identity information and Resource-Priority information, if available in the incoming request. The originating network shall include the signed information in the outgoing emergency request.

30. A network serving a UE receiving a PSAP call back shall, if configured though operator policies, invoke an AS for the verification of signed caller identity information, and Resource-Priority information, if available in the incoming request.

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 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

### 6.2.12 IBCF

- Forward emergency session establishment requests.

- Prioritize the emergency session based on operator policy.

- For an emergency session leaving an IBCF, the IBCF, if configured through operator policies, invokes an AS for the signing of attested caller identity and asserted Resource-Priority information, if available in the incoming request. The IBCF includes the signed information in the outgoing request.

- For a call back received by an IBCF, the IBCF, if configured through operator policies, shall invoke an AS for the verification of Resource-Priority information, if available in the incoming request.

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

## 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.

- A P-CSCF operating in a network that supports calling number attestation and signing may, based on operator policy, be responsible for inserting attestation information related to the asserted calling identity associated with an emergency session.

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

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

- A P-CSCF may assert Resource-Priority information for an emergency session, if configured through operator policies.

- 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: If 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.

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

## 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. Prior to forwarding the request to an appropriate E-CSCF, the P-CSCF may assert Resource-Priority information for an emergency session if configured through operator policies.

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]).

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

## 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.

- P-CSCF may, based on operator policy, insert attestation information related to the asserted calling identity associated with an emergency session, if operating in a network that supports calling number attestation and signing.

- P-CSCF may assert Resource-Priority information for an emergency session if configured through operator policies.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of changes \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*