**3GPP TSG-SA3 Meeting #100e *S3-201575-r2***

**e-meeting, 17 -28 August 2020**

|  |
| --- |
| *CR-Form-v12.0* |
| **CHANGE REQUEST** |
|  |
|  |  | **CR** |  | **rev** | **1**  | **Current version:** | **.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 |  |

|  |
| --- |
|  |
| ***Title:***  | Resolution of editor's note in clause 10.2.2.2 |
|  |  |
| ***Source to WG:*** | NTT DOCOMO |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | 5G\_Ph1-SEC |  | ***Date:*** | 2020-08-03 |
|  |  |  |  |  |
| ***Category:*** | F |  | ***Release:*** | Rel-15 |
|  | *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:*** | There is an editor's note in the description of emergency call setup stating it is FFS which message is being used to indicate authentication failure CT has defined which message is used to communicate authentication failure, so this editor's note can be resolved.  |
|  |  |
| ***Summary of change:*** | Reference to 24.501 and deletion of editor's note in clause 10.2.2.2 |
|  |  |
| ***Consequences if not approved:*** | Unresolved editor's note |
|  |  |
| ***Clauses affected:*** | 10.2.2.2 |
|  |  |
|  | **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:*** |  |

**Start of Changes**

#### 10.2.2.2 UE sets up an IMS Emergency session with emergency registration

UEs that are in limited service state (LSM) request emergency services by initiating the Registration procedure with the indication that the registration is to receive emergency services, referred to as Emergency Registration.

UEs that had earlier registered for normal services but now cannot be authenticated by the serving network, shall initiate Emergency Registration procedure to request emergency services.

It shall be possible to configure whether the network allows or rejects an emergency registration request and whether it allows unauthenticated UEs to establish bearers for unauthenticated IMS emergency sessions or not.

The AMF may attempt to authenticate the UE after receiving the emergency registration request.

If authentication failed in the UE during an emergency registration request, the UE shall wait for a NAS SMC command to set up an unauthenticated emergency bearer.

If authentication failed in the serving network and if the serving network policy does not allow unauthenticated IMS Emergency Sessions, the UE and AMF shall proceed as with the normal initial registration requests. The AMF shall reject the unauthenticated emergency bearer setup request from the UE.

If authentication failed in the serving network and if the serving network policy allow unauthenticated IMS Emergency Sessions, then the AMF shall support unauthenticated emergency bearer setup and the behaviours of the UE and the AMF are as described below.

a) UE behaviour:

After sending Emergency Registration request to the serving network the UE shall know of its own intent to establish an unauthenticated IMS Emergency Session.

The UE shall proceed as specified for the non-emergency case in except that the UE shall accept a NAS SMC selecting NEA0 and NIA0 algorithms from the AMF.

NOTE: In case of authentication success the AMF will send a NAS SMC selecting algorithms with a non-NULL integrity algorithm, and the UE will accept it.

b) AMF behavior:

After receiving Emergency Registration request from the UE, the AMF knows of that UE's intent to establish an unauthenticated IMS Emergency Session.

- If the AMF cannot identify the subscriber, or cannot obtain authentication vector (when SUPI is provided), the AMF shall send NAS SMC with NULL algorithms to the UE regardless of the supported algorithms announced previously by the UE.

- After the unsuccessful verification of the UE, the AMF shall send NAS SMC with NULL algorithms to the UE regardless of the supported algorithms announced previously by the UE.

- If both the Emergency Registration request and an AUTHENTICATION FAILURE message with error code as defined in 24.501 [35] clauses 5.4.1.2.4.5 (for EAP based authentication) or 5.4.1.3.7 (for 5G AKA based authentication) are received by the AMF from the UE, then the AMF shall send NAS SMC with NULL algorithms to the UE regardless of the supported algorithms announced previously by the UE.

If the UE has initiated a PDU session establishment procedure to establish bearers for unauthenticated IMS emergency sessions and the AMF has indicated to the SMF that this is an unauthenticated emergency call, then the SMF shall indicate 'Not Needed' in the UP security policy for both UP confidentiality and UP integrity protection to the ng-eNB/gNB.

**End of Changes**