**3GPP TSG-SA3 Meeting #116 *draft\_S3-242617-r1***

Jeju, South Korea, 20th - 24th May 2024

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  |  | **CR** | **2007** | **rev** | **0** | **Current version:** |  |  |
|  | | | | | | | | |
| *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:*** |  | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | vivo, China Telecom | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | TEI17 | | | | |  | ***Date:*** | | | 2024-05-13 |
|  |  | | | |  | |  | | |  |
| ***Category:*** |  |  | | | | | ***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 can be 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:*** | | The misalignment between the SA3 and RAN3 specifications may lead to backward compatibility issues for unauthenticated IMS sessions. According to clause 9.2.3.49 in TS 38.413, UE security capabilities shall include NIA, NEA, EIA, and EEA. While in 10.2.2.3.2 in TS 33.501, it is stated that "This implies that the source gNB will forward UE 5G security capability, which contains NIA0 and NEA0 only, to the target gNB."  Additionally, there is a mistake regarding unauthenticated IMS sessions: "A UE without a valid 5G subscription shall, at an IRAT handover to 5G, when an IMS Emergency Service is active, be considered by the AMF to be unauthenticated. In such a scenario, EIA0 shall be used in 5G after handover if the target network policy allows unauthenticated IMS Emergency Sessions." It is incorrect for gNB to configure EIA0 for NR PDCP, which may lead to confusion for operators regarding configuration.  It should be noted that SA3 has previously clarified gNB and ng-eNB actions, but for unauthenticated IMS sessions, it does not address that part. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | The following changes are made:   1. Align with RAN3 regarding the transmission of NIA0, NEA0, EIA0, and EEA0 in UE security capabilities. 2. Clarification of the distinct actions on gNB and ng-eNB for the utilization of the EIA0 component. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Misalignment between the SA3 and RAN3 specifications.  Incorrect guidance resulting wrong configuration of gNB/ng-eNB. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 6.7.3.6, 10.2.2.1, 10.2.2.3.2 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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 Change

10.2.2 Unauthenticated IMS Emergency Sessions

10.2.2.1 General

There are many scenarios when an unauthenticated Emergency Session may be established without the network having to authenticate the UE or apply ciphering or integrity protection for either AS or NAS. For example:

a) UEs that are in Limited service state UEs, as specified in clause 3.5 in TS 23.122

b) UEs that have valid subscription but SN cannot complete authentication because of network failure or other reasons

TS 23.401 clause 4.3.12.1 identifies four possible network behaviours of emergency bearer support. Amongst these, the following two cases are applicable for unauthenticated emergency sessions:

a. **IMSI required, authentication optional**. These UEs shall have a SUPI. If authentication fails, the UE is granted access and the unauthenticated SUPI retained in the network for recording purposes. The PEI is used in the network as the UE identifier. PEI only UEs will be rejected (e.g. UICCless UEs).

b. **All UEs are allowed**. Along with authenticated UEs, this includes UEs with a SUPI that cannot be authenticated and UEs with only an PEI. If an unauthenticated SUPI is provided by the UE, the unauthenticated SUPI is retained in the network for recording purposes. The PEI is used in the network to identify the UE.

The network policy is configured to one of the above, and accordingly determine how emergency requests from the UE are treated.

If the ME receives a NAS SMC selecting NIA0 (NULL integrity) for integrity protection, and NEA0 (NULL ciphering) for encryption protection, then:

- the ME shall mark any stored native 5G NAS security context on the USIM /non-volatile ME memory as invalid; and

- the ME shall not update the USIM/non-volatile ME memory with the current 5G NAS security context.

These two rules override all other rules regarding updating the 5G NAS security context on the USIM/non-volatile ME memory, in the present document.

If NIA0 is used, and the NAS COUNT values wrap around, and a new KAMF has not been established before the NAS COUNT wrap around, the NAS connection shall be kept.

NOTE: For unauthenticated IMS emergency sessions, NIA0, i.e., null integrity algorithm, is used for integrity protection. Additionally, as the NAS COUNT values can wrap around, the initialization of the NAS COUNT values are not crucial. Uplink and downlink NAS COUNT are incremented for NAS message that use NIA0, as for any other NAS messages.

A UE without a valid 5G subscription shall at an IRAT handover to 5G, when an IMS Emergency Service is active, be considered by the AMF to be unauthenticated. In such a scenario, NIA0 shall be used in 5G after handover if the target network policy allows unauthenticated IMS Emergency Sessions.

A handover from 5G to another RAT, of an unauthenticated IMS Emergency Session, shall result in an unauthenticated IMS Emergency Session in the other RAT.

Next of Change

10.2.2.3.2 Handover

When UE attempts to make Xn/N2 handover, UE and gNB derive and transfer the keys as normal to re-use the normal handover mechanism. Since the derived keys have no ability to affect the output of the NULL algorithms it is irrelevant that the network and the UE derive different keys. This implies that source gNB will forward UE 5G security capability which contains NIA0 and NEA0 to target gNB. So the target gNB can only select NIA0 for integrity protection and NEA0 for confidential protection. If the UE does not receive any selection of new AS security algorithms during a intra-gNB-CU handover, the UE continues to use the same algorithms as before the handover (see TS 38.331 [22]).

End of Change