**3GPP TSG-SA3 Meeting #104-e *S3-212796r3***

**e-meeting, 16 - 27 August 2021**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.501** | **CR** | **1182** | **rev** | **<3>** | **Current version:** | **17.2.1** |  |
|  | | | | | | | | |
| *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 |  | Core Network |  |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Security context handling in IRAT | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Apple, Qualcomm Incorporated | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | TEI17 | | | | |  | ***Date:*** | | | 2021-08-16 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **F** |  | | | | | ***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:*** | | When UE performs mobility between S1 and N1 mode, the current wording in TS 33.501 6.8.1.1.1 may leave UE in a state where there is no current 5G NAS security context but a valid non-current 5G NAS security context.  The scenario is:  STEP 1: UE has "native current EPS security context" while it camps and registered in LTE. While it also has a “current native 5G security context” from previous 5G registration.  STEP 2: UE moves from S1 to N1 via HO. NW indicated to use "mapped security context" (derived from current native EPS security context). So in this case UE is having "current mapped 5G security context” and "non-current native 5G security context”. (ref TS 33.501 Clause 8.4.2)  STEP 3: UE moves back from N1 to S1 in idle mode and uses "current mapped 5G security context” for integrity protection of TAU (ref 3GPP TS 33.501 subclause 8.5.2 step1). After TAU procedure, UE will delete "current mapped 5G security context” (ref 3GPP TS 33.501 subclause 8.5.2 ). At this time UE doesn’t have a current 5G security context but has one "non-current native 5G security context” as mentioned in STEP 2.  STEP4: While UE is in S1 mode, UE moves to EMM-DEREG state (e.g. due to power down detach). In this case UE operating in single registration mode will move to 5GMM-DEREG state as well. Whereas "non-current native 5G security context” won’t be stored in USIM because it has not upgraded to "current native 5G security context” for the condition described in TS 33.501 Clause 6.8.1.1.1.  When UE powers on and performs the Registration Request procedure, UE has to perform the AKA+ SMC procedure to derive a new security context, which could cause approximately 30% delay and thus impact the KPI of the registration time. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | On deleting the mapped 5G context at successful interworking from 5G to 4G, the UE makes a full non-current native 5G NAS security context into the current security context if such a non-current native 5G NAS security context exists. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | There will be approximately 30% delay in UE’s registration request procedure. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 8.3.2, 8.5.2 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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 \*\*\*\***

8.3.2 Procedure

****

**Figure 8.3.2-1 Handover from 5GS to EPC over N26**

NOTE 1: This procedure is based on clause 4.11.1.2.1 in TS 23.502 and only includes steps and description that are relevant to security.

If the UE is initially registered and connected to the 5GC, the 5GC has a current security context for the UE. The current 5G security context may be a mapped 5G security context resulting from a previous mobility from EPC, or a native 5G security context resulting from a primary authentication with the 5GC.

1. The gNB/ng-eNB sends a Handover Required message to the AMF, including UE’s identity .

2. When the source AMF performs a handover procedure to the EPC, after checking the UE's access rights and security capabilities, the source AMF shall prepare a UE context including a mapped EPS security context for the target MME. To construct the mapped EPS security context, the source AMF shall derive a K’ASME using the KAMF key and the current downlink 5G NAS COUNT of the current 5G security context as described in clause 8.6.1 and then increments its stored downlink 5G NAS COUNT value by one.

The source AMF shall select the EPS NAS algorithms identifiers (it has stored) to be used in the target MME at interworking handover to EPS, for encryption and integrity protection.

NOTE 2: A legacy target MME is expecting to receive the selected EPS NAS algorithms identifiers over N26 from the source AMF as the target MME believes the source AMF is another MME. The source AMF has therefore provisioned the EPS NAS security algorithms identifiers to be used at interworking handover to EPS to the UE in the 5G NAS SMC in 5G access as described in clause 6.7.2. The target MME could re-select different EPS NAS algorithms though to be used with the UE by running a NAS SMC in the following Tracking Area Update procedure.

The uplink and downlink EPS NAS COUNT associated with the newly derived KASME' key are set to the values as described in clause 8.6.1. The eKSI for the newly derived KASME' key is defined as described in clause 8.6.1.

The source AMF shall also derive the initial KeNB key from the KASME' key and the uplink NAS COUNT as specified in Annex A.3 of TS 33.401 [10] using 232-1 as the value of the uplink NAS COUNT parameter.

NOTE 3: The source AMF and the UE only uses the 232-1 as the value of the uplink NAS COUNT for the purpose of deriving KeNB and do not actually set the uplink NAS COUNT to 232-1. The reason for choosing such a value not in the normal NAS COUNT range, i.e., [0, 224-1] is to avoid any possibility that the value may be used to derive the same KeNB again.

The source AMF subsequently derives NH two times as specified in clause A.4 of TS 33.401 [10]. The {NH, NCC=2} pair is provided to the target MME as a part of UE security context in the Forward Relocation Request message.

3. The source AMF shall transfer the UE security context (including new KASME', eKSI, uplink and downlink EPS NAS COUNT’s, UE EPS security capabilities, selected EPS NAS algorithms identifiers) to the target MME in the Forward Relocation Request message. The UE NR security capabilities may be sent by the source AMF as well.

4. When the target MME receives Forward Relocation Request message from source AMF, then the target MME shall derive EPS NAS keys (i.e., KNASenc and KNASint) from the received KASME' key with the received EPS NAS security algorithm identifiers as input, to be used in EPC as described in Annex A.7 in TS 33.401 [10]. The target MME needs to include the {NH, NCC=2} pair and the UE security capabilities in the S1 HANDOVER REQUEST message to the target LTE eNB. The UE security capabilities include the UE EPS security capabilities received from the source AMF.

5. Upon receipt of the S1 HANDOVER REQUEST from the target MME, the target LTE eNB selects AS security algorithmsfrom the UE EPS security capabilities as described in clause 7.2.4.2.3 in TS 33.401 [10] and computes the KeNB to be used with the UE and proceed as described in clause 7.2.8.4.3 in TS 33.401[10]. The target LTE eNB then sends the selected AS security algorithms in the target to source transparent container in the S1 Handover Request Ack Message to the target MME.

6. The target MME shall include the target to source transparent container received from the target LTE eNB in the Forward Relocation Response message sent to the source AMF.

7. The source AMF shall include the target to source transparent container and the 8 LSB of the downlink NAS COUNT value used in KASME’ derivation in step 2, in the Handover command sent to the source gNB/ng-eNB.

8. The source gNB/ng-eNB shall include the target to source transparent container and the 8 LSB of the downlink NAS COUNT value in the Handover command sent to the UE.

Upon the reception of the Handover Command message, the UE shall estimate the downlink NAS COUNT value using the received 8 LSB of the downlink NAS COUNT value and its stored downlink NAS COUNT value. The UE shall ensure that the estimated downlink NAS COUNT value is greater than the stored downlink NAS COUNT value. Then, the UE shall derive the mapped EPS security context, i.e. derive KASME' from KAMF as described in clause 8.6.1 using the estimated downlink 5G NAS COUNT value. After the derivation the UE shall set the downlink NAS COUNT value in the 5G NAS security context to the received downlink NAS COUNT value.

9. The eKSI for the newly derived KASME' key is defined as described in clause 8.6.1. The UE shall also derive the EPS NAS keys (i.e. KNASenc and KNASint) as the MME did in step 4 using the EPS NAS security algorithms identifiers stored in the ME and provisioned by the AMF to the UE in 5G NAS SMC in earlier 5G access. The UE shall also derive the initial KeNB from the KASME' and the uplink NAS COUNT as specified in Annex A.3 of TS 33.401 [10] using 232-1 as the value of the uplink NAS COUNT parameter.

The UE shall also derive the {NH, NCC=2} pair as described in A.4 of TS 33.401 [10] and further derive the KeNB to be used with the UE by performing the key derivation defined in Annex A.5 in TS 33.401[10]. The UE shall derive the AS RRC keys and the AS UP keys based on the KeNB and the received AS EPS security algorithms identifiers selected by the target eNB as described in Annex A.7 in TS 33.401 [10]. The uplink and downlink EPS NAS COUNT associated with the derived EPS NAS keys are set to the values as described in clause 8.6.1. The UE shall immediately take into use the newly created mapped EPS security context, both for NAS and AS communication.

10. The UE sends the Handover Complete message to the target LTE eNB. The UE shall cipher and integrity protect this message using the newly created mapped EPS security context.

11. The target LTE eNB notifies the target MME with a Handover Notify message.

After successful completion of the Handover procedure, the UE shall delete any mapped 5G security context. After deleting the mapped 5G security context, if the UE has a full non-current native 5G NAS security context then the UE shall make the non-current native 5G NAS security context the current one.

**\*\*\*\* NEXT CHANGE \*\*\*\***

8.5.2 TAU Procedure

NOTE: This procedure is based on clause 4.11.1.3.2 in TS 23.502 [8] and only includes steps and descriptions that are relevant to security.

****

**Figure 8.5.2-1: Idle mode mobility from 5G to 4G**

1. The UE initiates the TAU procedure by sending a TAU Request to the MME with a mapped EPS GUTI derived from the 5G GUTI and its EPS security capabilities. The mapped EPS GUTI contains the information of the AMF that has the latest UE context in the 5G network.

The UE integrity protects the TAU Request message using the current 5G NAS security context identified by the 5G GUTI used to derive the mapped EPS GUTI. More precisely, the UE shall compute the NAS MAC for the TAU request as it is done for a 5G NAS message over a 3GPP access. The NAS Uplink COUNT for integrity protection of the TAU request shall use the same value as the 5G NAS Uplink COUNT. Consequently, this results in an increase of the stored NAS Uplink COUNT value in the NAS COUNT pair associated with the 3GPP access. The corresponding ngKSI value of the 5G Security context is included in the eKSI parameter of the TAU Request message.

2. Upon receipt of the TAU Request, the MME obtains the AMF address from the mapped EPS GUTI value.

3. The MME forwards the complete TAU Request message including the eKSI, NAS-MAC and mapped EPS GUTI in the Context Request message.

4. The AMF shall use the eKSI value field to identify the 5G NAS security context and use it to verify the TAU Request message as if it was a 5G NAS message received over 3GPP access.

5. If the verification is successful, the AMF shall derive a mapped EPS NAS security context as described in clause 8.6.1. The AMF shall set the EPS NAS algorithms to the ones indicated earlier to the UE in a NAS SMC as described in clause 6.7.2.

The AMF shall include the mapped EPS NAS security context in the Context Response message it sends to the MME. The AMF shall never transfer 5G security parameters to an entity outside the 5G system.

6. The UE shall derive a mapped EPS NAS security context as described in clause 8.6.1. The UE shall select the EPS algorithms using the ones received in an earlier NAS SMC from the AMF as described in clause 6.7.2. The UE shall immediately activate the mapped EPS security context and be ready to use it for the processing of the TAU Accept message in step 7.

7. The MME compares the UE security algorithms to its configured list after it receives the Context Response message. If an algorithm change is required, the MME shall select the NAS algorithm which has the highest priority from its configured list and is also present in the UE 5G security capabilities and initiate an NAS SMC to the UE. Otherwise, step 8~10 shall be skipped.

8 - 10. The MME and the UE performs an NAS SMC to derive new NAS keys with the new algorithms as described in Clause 7.2.8.1.2 of TS 33.401[10].

11. The MME completes the procedure with a TAU Accept message.

After successful completion of the TAU procedure, the UE shall delete any mapped 5G security context. After deleting the mapped 5G security context, if the UE has a full non-current native 5G NAS security context then the UE shall make the non-current native 5G NAS security context the current one.

**\*\*\*\* END OF CHANGES \*\*\*\***