**3GPP TSG-SA3 Meeting #98e S3-200220 e-meeting, 2 – 6 March 2020**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v11.4* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.501** | **CR** | **0741** | **rev** | **1** | **Current version:** | **15.7.0** |  |
|  | | | | | | | | |
| *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:*** | Clarification on native 5G NAS security context activation after an inter-system change from S1 mode to N1 mode in idle mode in Rel15 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Huawei, Hisilicon | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | 5GS\_Ph1-SEC | | | | |  | ***Date:*** | | | 2020-3-2 |
|  |  | | | |  | |  | | |  |
| ***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 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-12 (Release 12)* *Rel-13 (Release 13) Rel-14 (Release 14) Rel-15 (Release 15) Rel-16 (Release 16)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | According to the LS S3-192279, SA3 has informed CT1 that for subsequent NAS signalling message after an inter-system change from S1 mode to N1 mode in idle mode , it is up to AMF when to activate the native 5G security context. Hence, the AMF is recommended to activate the native KAMF by performing a NAS SMC procedure.  However, currently, TS 33.501 subclause 8.4.2 step 10 illustrated that  "The AMF shall retrieve the native security context using the 5G GUTI. The AMF shall activate the native KAMF by performing a NAS SMC procedure."  Meanwhile, the above misalignment is inquired by LS C1-199003 from CT1. Therefore, it is recommended to change the “shall” to “is recommended to”. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Change “The AMF shall activate the native KAMF by performing a NAS SMC procedure.” to “The AMF determines to activate the native KAMF by performing a NAS SMC procedure based on its local policy.” | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | There would be misalignment between LS S3-192279 and TS 33.501. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 8.4.2 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | |  | | | | | | | | |

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

### 8.4.2 Procedure



Figure 8.4.2-1: Handover from EPS to 5GS over N26

NOTE 1: This procedure is based on clause 4.11.1.2.2 in TS 23.502 [8] and only includes steps and description that are relevant to security.

As the UE is connected to the EPS, the source MME has a current EPS security context for the UE. The current EPS security context may be a mapped EPS security context resulting from a previous mobility from 5GC, or a native EPS security context resulting from a primary authentication with the EPS.

1. The source eNB sends a Handover Required message to the source MME, including UE's identity .

NOTE 2: The source MME checks whether the UE's security capabilities and access rights are valid in order to decide whether it can initiate handover to 5GS.

2. The source MME selects the target AMF and sends a Forward Relocation Request to the selected target AMF. The source MME includes UE's EPS security context including KASME, eKSI, UE EPS security capabilities, selected EPS NAS algorithm identifiers, uplink and downlink EPS NAS COUNTs, {NH, NCC} pair, in this message. If the source MME has the UE NR security capabilities stored, then it will forward the UE NR security capabilities as well to the target AMF.

3. The target AMF shall construct a mapped 5G security context from the EPS security context received from the source MME. The target AMF shall derive a mapped KAMF key from the received KASME and the NH value in the EPS security context received from the source MME as described in clause 8.6.2.

If the target AMF receives the UE 5G security capabilities, then the target AMF shall select the 5G NAS security algorithms (to be used in the target AMF for encryption and integrity protection) which have the highest priority from its configured list.

If the target AMF does not receive the UE 5G security capabilities from the source MME, then the target AMF shall assume that the following default set of 5G security algorithms are supported by the UE (and shall set the UE 5G security capabilities in the mapped 5G NAS security context according to this default set):

a. NEA0, 128-NEA1 and 128-NEA2 for NAS signalling ciphering, RRC signalling ciphering and UP ciphering;

b. 128-NIA1 and 128-NIA2 for NAS signalling integrity protection, RRC signalling integrity protection and UP integrity protection.

The target AMF then derives the complete mapped 5G security context. The target AMF shall derive the 5G NAS keys (i.e., KNASenc and KNASint) from the new KAMF' with the selected 5G NAS security algorithm identifiers as input, to be used in AMF as described in clause A.8. The uplink and downlink 5G NAS COUNTs associated with the derived 5G NAS keys are set to the value as described in clause 8.6. 2. The ngKSI for the newly derived KAMF' key is defined such as the value is taken from the eKSI of the KASME key (i.e. included in the received EPS security context) and the type is set to indicate a mapped security context. The target AMF shall store the EPS NAS security algorithms received from the source MME in the mapped 5G security context. Similar to N2-Handover defined in Clause 6.9.2.3.3, the target AMF shall also set the NCC to zero and shall further derive the temporary KgNB using the mapped KAMF' key and the uplink NAS COUNT value of 232-1 as specified in Annex A.9.

The target AMF associates this mapped 5G Security context with ngKSI.

NOTE 3: The target AMF derives a temporary KgNB using the mapped KAMF instead of using the {NH, NCC} pair received from the MME. The uplink NAS COUNT value for the initial KgNB derivation is set to 232-1. The reason for choosing such a value is to avoid any possibility that the value may be used to derive the same KgNB again.

The target AMF shall create a NAS Container to signal the necessary security parameters to the UE. The NAS Container shall include a NAS MAC, the selected 5G NAS security algorithms, the ngKSI associated with the derived KAMF' and the NCC value associated with the NH parameter used in the derivation of the KAMF'. The target AMF shall calculate the NAS MAC as described in clause 6.9.2.3.3. with the COUNT parameter set to the maximal value of 232-1.

4. The target AMF requests the target gNB/ng-eNB to establish the bearer(s) by sending the Handover Request message.

The target AMF sends the NAS Container created in step 3 along with, the {NCC=0, NH=derived temporary KgNB}, the New Security Context Indicator (NSCI), and the UE security capabilities in the Handover Request message to the target gNB/ng-eNB. The target AMF shall further set the NCC to one and shall further compute a NH as specified in Annex A.10. The target AMF shall further store the {NCC=1, NH} pair.

5. The target gNB/ng-eNB shall selects the 5G AS security algorithms from the list in the UE security capabilities

The target gNB/ng-eNB shall compute the KgNB to be used with the UE by performing the key derivation defined in Annex A.11 with the {NCC, NH} pair received in the Handover Request message and the target PCI and its frequency ARFCN-DL. The target gNB/ng-eNB shall associate the NCC value received from AMF with the KgNB.The target gNB /ng-eNB shall then derive the 5G AS security context, by deriving the 5G AS keys (KRRCint, KRRCenc, KUPint, and KUPenc) from the KgNB and the selected 5G AS security algorithm identifiers as described in Annex A.8 for gNB and in Annex A.7 in TS 33.401[10].

The target gNB/ng-eNB sends a Handover Request Ack message to the target AMF. Included in the Handover Request Ack message is the Target to Source Container, which contains the selected 5G AS algorithms, the *keySetChangeIndicator*, the NCC value from the received {NH, NCC} pair, and the NAS Containerreceived from the target AMF. If the target gNB/ng-eNB had received the NSCI, it shall set the *keySetChangeIndicator* field to true, otherwise it shall set the *keySetChangeIndicator* field to false.

6. The target AMF sends the Forward Relocation Response message to the source MME. The required security parameters obtained from gNB/ng-eNB in step 5 as the Target to Source Container are forwarded to the source MME.

7. The source MME sends the Handover Command to the source eNB. The source eNB commands the UE to handover to the target 5G network by sending the Handover Command. This message includes all the security related parameters in the NAS Container obtained from the target AMF in step 6.

8. The UE derives a mapped KAMF' key from the KASME in the same way the AMF did in step 3. It shall also derive the 5G NAS keys and KgNB corresponding to the AMF and the target gNB/ng-eNB in step 3 and step 5. The UE shall further set the selected EPS NAS security algorithms in the 5G security context to the NAS security algorithms used with the source MME. It associates this mapped 5G security context with the ngKSI included in the NAS Container. The UE shall verify the NAS MAC in the NAS Container.

If verification of the NAS MAC fails, the UE shall abort the handover procedure. Furthermore, the UE shall discard the new NAS security context if it was derived and continue to use the existing NAS and AS security contexts.

NOTE 4: Void.

The mapped 5G security context shall become the current 5G security context.

9. The UE sends the Handover Complete message to the target gNB/ng-eNB. This shall be ciphered and integrity protected by the AS keys in the current 5G security context.

10. The target gNB/ng-eNB notifies the target AMF with a Handover Notify message.

If the UE has a native 5G security context established during the previous visit to 5GS, then the UE shall provide the associated the 5G GUTI as an additional GUTI in the Registration Request following the handover procedure. The UE shall use the mapped 5G security context to protect the subsequent Registration Request message over 3GPP access. The target AMF shall validate the integrity of the Registration Request message using the mapped security context. Upon successful validation, the target AMF shall send a context request message to the old AMF and shall include the additional GUTI and an indication that the UE is validated. Upon receiving the context request message with the indication that the UE is validated, the old AMF shall skip the integrity check and transfer the native 5G security context to the target AMF.The AMF shall retrieve the native security context using the 5G GUTI. If the AMF determines to activate the native security context, the AMF shall perform a NAS SMC procedure.

NOTE x: It is up to AMF when to activate the native 5G security context.

If the handover is not completed successfully, the new mapped 5G security context cannot be used in the future. In this case, the AMF shall delete the new mapped 5G security context.

If the AMF has no native 5G security context available when the UE performs the Registration Request (protected by the mapped 5G security context) following the handover procedure, then the AMF via the SEAF should run a primary authentication depending on local operator policy.

The handling of security contexts in the case of multiple active NAS connections in the same PLMN’s serving network is given in clasue 6.4.2.2.

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