**3GPP TSG-SA3 Meeting #102-e *S3-21aabb***

**e-meeting, 18 - 29 January 2021, Online was S3-210326**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.501** | **CR** | **1041** | **rev** | **1** | **Current version:** | **16.5.0** |  |
|  | | | | | | | | |
| *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:*** | Correct current uplink EPS NAS COUNT used at derivation of a mapped 5G security context | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | MediaTek Inc. | | | | | | | | | |
| ***Source to TSG:*** | SA3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | TEI16 | | | | |  | ***Date:*** | | | 2021-01-29 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **F** |  | | | | | ***Release:*** | | | Rel-16 |
|  | *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:*** | | Quotation from 33.501:  **"*8.2 Registration procedure for mobility from EPS to 5GS over N26***  *• If the UE has no current 5G security context then the UE shall send the Registration Request message without integrity protection. The Registration*  *Request shall contain the TAU request integrity protected using the EPS NAS security context shared with the source MME as it is performed for a*  *LTE NAS message, then the UE shall increment its stored uplink EPS NAS COUNT value by one.*"  As specified in 8.2, the UE shall increment uplink EPS NAS COUNT value (i.e. the sequence number of the COUNT) by one when the UE creates and encloses TAU Request in the Registration Request.  Quotation from 33.501:  **"*8.6.2 Mapping of an EPS security context to a 5G security context***  *• The derivation of a mapped 5G security context from an EPS security is done as described below*  * The KAMF' key, taken as the KAMF, shall be derived from the KASME using the current EPS NAS Uplink COUNT in idle mode mobility or the NH*  *value in handovers as described in clause A.15*"  As specified in 8.6.2 "current EPS NAS Uplink COUNT" shall be used for KAMF' from KASME derivation. However, it's not clearly specified that the current uplink EPS NAS COUNT used for mapped 5G security context derivation shall be derived from the sequence number of the TAU request message included in the REGISTRATION REQUEST message.  It shall be specified that the network shall use the uplink EPS NAS COUNT indicated in the received TAU Request message. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | It is clarified that for the derivation of mapped 5GS security context from EPS security context the network shall use the uplink EPS NAS count of the TAU Request message that was included in the Registration Request. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Connection failure if the UE and the network are using different EPS NAS uplink COUNT in the derivation of KAMF' from KASME. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 8.2 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | |  | | | | | | | | |

### 

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

## 8.2 Registration procedure for mobility from EPS to 5GS over N26

During mobility from EPS to 5GS, the security handling described below shall apply.

When the UE performs idle mode mobility from EPS to 5GS, and if the UE has a native non-current 5G context, then the UE shall make the native non-current 5G context as the current one. The UE shall discard any mapped 5G security context.

The UE shall include the UE 5G security capability alongside the mapped 5G GUTI in the Registration Request message. The UE shall also include the 5G GUTI and the ngKSI that identify a current 5G security context if available, e.g. established during an earlier visit to 5G, and integrity protect the Registration Request using the selected security algorithms in the current 5G NAS security context as it is performed for a 5G NAS message over a 3GPP access. If the UE has no current 5G security context then the UE shall send the Registration Request message without integrity protection.The Registration Request shall contain the TAU request integrity protected using the EPS NAS security context shared with the source MME as it is performed for a LTE NAS message, then the UE shall increment its stored uplink EPS NAS COUNT value by one.

NOTE: The enclosed TAU request in the Registration Request contains a complete TAU Request.

Upon receipt of the Registration Request, the AMF shall interact with the MME identified by the mapped 5G GUTI to retrieve the UE context. The AMF shall include the enclosed TAU request in the Context Request message to the MME. The MME shall verify the TAU request using the stored UE security context and if the verification is successful, the MME shall send the UE context to the AMF.

The AMF shall verify the integrity of the Registration Request message if the AMF obtained the 5G security context identified by the 5G GUTI. In case the verification succeeds then the AMF shall then dispose of any EPS security parameters received from the source MME in the Context Response message. In case the verification fails or the 5G UE context is not available then the AMF shall treat the Registration Request message as if it was unprotected. In such case, the AMF may either derive a mapped 5G security context from the EPS context received from the source MME as described in clause 8.6.2 or initiate a primary authentication procedure to create a new native 5G security context.

If the AMF derives a mapped 5G security context from the EPS security context, then the ngKSI associated with the newly derived mapped 5G security context and the uplink and downlink 5G NAS COUNTs are defined and set as described in clause 8.6.2. If the Registration Request contains a TAU Request message, the network shall use the uplink EPS NAS COUNT corresponding to the TAU Request message for deriving the KAMF' from the KASME. The AMF shall use and include the ngKSI to the UE in NAS SMC procedure, for the UE to identify the EPS security context used for the derivation of a mapped 5G security context. If a mapped 5G security context is created or the native 5G security context has been changed (e.g., due to a new KAMF' derivation or NAS algorithm change), the AMF shall activate the resulting 5G security context by a NAS SMC procedure. When a mapped 5G security context is created, the AMF shall store the selected EPS NAS security algorithms in the mapped 5G security context and include them in the NAS Security Mode Command.

If the AMF wants to continue to use the native 5G security context used by the UE to protect the Registration Request, the AMF may skip the NAS SMC procedure and send the Registration Accept message protected using the native 5G security context identified by the 5G-GUTI and the ngKSI included in the Registration Request message.

In case the type value in the received ngKSI in NAS SMC indicates a mapped security context, then the UE shall use the value field in the received ngKSI to identify the EPS security context from which the UE derives the mapped 5G security context as described in clause 8.6.2. The UE shall activate the mapped 5G security context to verify the integrity protection of the NAS SMC as it is performed for a 5G NAS message over a 3GPP access.

The Registration Accept message shall be protected by the new mapped 5G security context (if a mapped 5G security context was activated by NAS SMC) or by the new native 5G security context (if a new native 5G security context was activated by NAS SMC) as it is performed for a 5G NAS message over a 3GPP access. Otherwise, the current native 5G security context shall be used. If the AMF chooses to derive an initial KgNB from a new KAMF key (either the mapped KAMF' key or the native KAMF key), then the initial KgNB is derived as specified in Annex A.9 using the start value of the uplink 5G NAS COUNT protecting the NAS Security Mode Command Complete message and an access type distinguisher set to "3GPP access". If the UE receives an AS SMC message, then the UE shall derive an initial KgNB from a new KAMF key in the same way as the AMF.