**3GPP TSG-SA3 Meeting #103-e *draft\_S3-211874-r1***

**e-meeting, 17th - 28th May 2021**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.501** | **CR** | 1119 | **rev** |  | **Current version:** | **16.6.0** |  |
|  | | | | | | | | |
| *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:*** | Solving misalignment on mapped security derivation | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Huawei, HiSilicon | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | TEI16 | | | | |  | ***Date:*** | | | 2021-05-10 |
|  |  | | | |  | |  | | |  |
| ***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-12 (Release 12)* *Rel-13 (Release 13) Rel-14 (Release 14) Rel-15 (Release 15) Rel-16 (Release 16)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | In SA3#102e meeting, contribution SA3-210787 was agreed which clarifies that in idle mobility from EPS to 5GS, the network shall use the uplink EPS NAS COUNT corresponding to the TAU Request message included in the Registration Request (RR) message for deriving the KAMF' from the KASME, if the RR contains a TAU Request message and the network decides to derive the mapped 5GS security context.  There are sill some clauses in current 33.501 which do not align with the above agreed contribution. This contribuiton proposes to fix this. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Modification to clause 8.6.2 (i.e. Mapping of an EPS security context to a 5G security context) and Annex A.15 (KASME to KAMF' derivation for interworking), to align with the agreed contribution. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Inconsistency in TS 33.501 | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 8.6.2, Annex A.15 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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 1\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of Change 1 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

### 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 EPS NAS Uplink COUNT of the TAU message included in the Registration Request message in idle mode mobility or the NH value in handovers as described in clause A.15.

- The ngKSI for the newly derived KAMF key shall be defined such as the value field is taken from the eKSI and the type field is set to indicate a mapped security context.

- The 5G NAS COUNT values in the mapped 5G security context shall be set to 0.

NOTE: The selection of the 5G NAS algorithms is performed by the AMF and signalled to the UE either in the NAS Container during handovers as described in clause 8.4, or in a NAS SMC during idle mode mobility as described in clause 8.2.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of Change 2\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

# A.15 KASME to KAMF' derivation for interworking

## A.15.1 Idle mode mobility

This input string is used when there is a need to derive KAMF' from KASME during mapping of security contexts from EPS to 5G at idle mode mobility. The following input parameters shall be used.

- FC = 0x75

- P0 = NAS Uplink COUNT value of the TAU message included in the Registration Request message

- L0 = length of NAS Uplink COUNT value of the TAU message included in the Registration Request message (i.e. 0x00 0x04)

The input key KEY shall be KASME.

### A.15.2 Handover

This input string is used when there is a need to derive KAMF' from KASME during mapping of security contexts from EPS to 5G at handovers. The following input parameters shall be used.

- FC = 0x76

- P0 = NH value

- L0 = length of NH value (i.e. 0x00 0x20)

The input key KEY shall be KASME.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of Change 2 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*