**3GPP TSG-CT WG6 Meeting #89-Bis *C6-180408***

**Sophia Antipolis, France, 10th July – 13th July 2018**

|  |
| --- |
| *CR-Form-v11.1* |
| **CHANGE REQUEST** |
|  |
|  | **31.102** | **CR** | **0810** | **rev** | **1** | **Current version:** | **15.1.0** |  |
|  |
| *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 | **X** | ME | **X** | Radio Access Network |  | Core Network |  |

|  |
| --- |
|  |
| ***Title:***  | Correct Kseaf and Kausf length in EF5GAUTHKEYS to align with SA3 specification |
|  |  |
| ***Source to WG:*** | Qualcomm Incorporated |
| ***Source to TSG:*** | C6 |
|  |  |
| ***Work item code:*** |  |  | ***Date:*** | 2018-07-13 |
|  |  |  |  |  |
| ***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 canbe 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:*** | Kseaf and Kausf lengths are specified incorrectly as 128 bits. Per TS 33.501 (clause A.7 for example), the keys are 256 bits long. |
|  |  |
| ***Summary of change:*** | Kseaf and Kausf lengths in EF5GAUTHKEYS are changed from 16 bytes to 32 bytes. |
|  |  |
| ***Consequences if not approved:*** | ME is unable to store Kseaf and Kausf in the USIM even if the corresponding EF is present on the USIM. |
|  |  |
| ***Clauses affected:*** | 4.2.114 |
|  |  |
|  | **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:*** |  |

### 4.2.114 EF5GAUTHKEYS (5G authentication keys)

If Service n°123 is "available", this file shall be present.

This EF contains KAUSF and KSEAF that are generated on the ME using CK and IK as part of AKA procedures as described in TS 33.501 [105].

|  |  |  |
| --- | --- | --- |
| Identifier: '6F01' | Structure: transparent | Optional |
| File size: >= 68 bytes | Update activity: high |
| Access Conditions: READ PIN UPDATE PIN DEACTIVATE ADM ACTIVATE ADM |
| Description | Value | M/O | Length |
| KAUSF Tag | '80' | M | 1 |
| Length | K (Note2) | M | Note1 |
| KAUSF | -- | M | K (Note2) |
| KSEAF Tag | '81' | M | 1 |
| Length | L (Note2) | M | Note1 |
| KSEAF | -- | M | L (Note2) |
| Note 1: The length is coded according to ISO/IEC 8825-1 [35] |
| Note 2: As per TS 33.501 [105], the length of keys KAUSF and KSEAF is 32 bytes each |

‑ KAUSF Tag '80'.

Contents:

- KAUSF as described in TS 33.501[105]).

Coding:

- The most significant bit of KAUSF is the most significant bit of the 1st byte of this TLV value field. The least significant bit of KAUSF is the least significant bit of the last byte of this TLV value field.

‑ KSEAF Tag '81'.

Contents:

- KSEAF as described in TS 33.501[105]).

Coding:

- The most significant bit of KSEAF is the most significant bit of the 1st byte of this TLV value field. The least significant bit of KSEAF is the least significant bit of the last byte of this TLV value field.