**3GPP TSG-SA3 Meeting #101-e *S3-203029***

**e-meeting, 9th - 20th November 2020**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.535** | **CR** | **0050** | **rev** |  | **Current version:** | **16.1.0** |  |
|  | | | | | | | | |
| *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:*** | Storage of the AKMA keys in the UE. | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Thales | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | AKMA | | | | |  | ***Date:*** | | | 28/10/2020 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | B |  | | | | | ***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-12 (Release 12)* *Rel-13 (Release 13) Rel-14 (Release 14) Rel-15 (Release 15) Rel-16 (Release 16)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | The description of the storage in the UE of the AKMA keys (KAKMA and KAF) is missing. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | The ME shall store the AKMA keys (KAKMA and KAF) in the USIM if the USIM supports the AKMA keys storage. If the USIM does not support the AKMA keys storage, then the ME shall store the AKMA keys in the ME non-volatile memory.  The storage of the AKMA keys in the USIM is optional and depends on configuration of the USIM performed by the home network operator.  Such a mechanism is already specified in 3GPP TS 33.501 to optionally store the key KAUSF in the USIM. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | The description of the storage of the AKMA keys (KAKMA and KAF) in the UE is missing.  If the AKMA keys are not stored in the USIM then there are scenarios where the AKMA keys previously established are no longer available in the UE. Consequently, new AKMA keys (KAKMA and KAF) shall be re-established between the UE, the AKMA Anchor Function and the Application Functions. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 5.1 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | |  | | | | | | | | |

## 

## 5.1 AKMA key hierarchy

The key hierarchy (see Figure 5.1-1) includes the following keys: KAUSF, KAKMA, KAF. KAUSF is generated by AUSF as specified in clause 6 of TS 33.501 [2].

Keys for AAnF:

- KAKMA is a key derived by ME and AUSF from KAUSF.

- The ME shall store KAKMA in the USIM if the USIM supports the AKMA keys storage. If the USIM does not support the AKMA keys storage, then the ME shall store the AKMA keys in the ME non-volatile memory.

Keys for AF:

- KAF is a key derived by ME and AAnF from KAKMA.

- The ME shall store KAF on the USIM if the USIM supports the AKMA keys storage. If the USIM does not support the AKMA keys storage, then the ME shall store the AKMA keys in the ME non-volatile memory.

KAKMA and KAF are derived according to the procedures of clauses 6.1 and 6.2.



Figure 5.1-1: AKMA Key Hierarchy derivation