**3GPP TSG-SA3 Meeting #100e *S3-201946r1***

**e-meeting, 17 - 28 August 2020**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  |  | **CR** |  | **rev** | **1** | **Current version:** |  |  |
|  | | | | | | | | |
| *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 | **X** | Radio Access Network |  | Core Network | **X** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Assignment of FC values for key derivations | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Qualcomm Incorporated, China Mobile | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** |  | | | | |  | ***Date:*** | | | 06-08-2020 |
|  |  | | | |  | |  | | |  |
| ***Category:*** |  |  | | | | | ***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:*** | | Need to assign FC values to the AKMA TS | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Assign AKMA values to the AKMA TS | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | AKMA key derivations are not fully standardised | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | A.1.2, A.2, A.3, A.4 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **Y** | **N** |  | | | |  | | |
| ***Other specs*** | | **x** |  | Other core specifications | | | | TS 33.220 CR 0203 | | |
| ***affected:*** | |  | **x** | Test specifications | | | | TS/TR ... CR ... | | |
| ***(show related CRs)*** | |  | **x** | O&M Specifications | | | | TS/TR ... CR ... | | |
|  | |  | | | | | | | | |
| ***Other comments:*** | | This CR should only be approved if the related CR is approved | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | | Rev 1: merged with S3-201786 | | | | | | | | |

**\*\*\*\* START OF CHANGES \*\*\*\***

A.1.2 FC value allocations

The FC number space used is controlled by TS 33.220 [4], FC values allocated for the present document are in the range of 0x80 – 0x82.

A.2 KAKMA derivation function

When deriving a KAKMA from KAUSF, the following parameters shall be used to form the input S to the KDF:

- FC = 0x80;

- P0 = "AKMA";

- L0 = length of "AKMA"; (i.e. 0x00 0x04)

- P1 = SUPI;

- L1 = length of SUPI.

The input key KEY shall be KAUSF.

A.3 A-TID derivation function

When deriving the A-TID from KAUSF, the following parameters shall be used to form the input S to the KDF:

- FC = 0x81;

- P0 = "A-TID";

- L0 = length of "A-TID"; (i.e. 0x00 0x05)

- P1 = SUPI;

- L1 = length of SUPI.

The input key KEY shall be KAUSF.

A.4 KAF derivation function

When deriving a KAF from KAKMA, the following parameters shall be used to form the input S to the KDF:

- FC = 0x82;

- P0 =AF\_ID;

- L0 = length of AF\_ID

The input key KEY shall be KAKMA.

**\*\*\*\* END OF CHANGES \*\*\*\***