**3GPP TSG-SA3 Meeting #100e *S3-201977-r1***

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

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.501** | **CR** | **0937** | **rev** | **1** | **Current version:** | **16.3.0** |  |
|  | | | | | | | | |
| *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 | **X** | Radio Access Network | **X** | Core Network |  |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Allocation of FC values for KIAB derivation function | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Samsung | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | IAB | | | | |  | ***Date:*** | | | 03-08-2020 |
|  |  | | | |  | |  | | |  |
| ***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:*** | | Allocation of a Function Code value for KIAB key derivation function is needed to derive cryptographically unique keys. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Allocation of FC value for KIAB key derivation function. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Possible allocation of a FC value to more than one key derivation function which breaks the desired security property. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | A.23 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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 should only be approved if the related CR (S3-20xxxx) is approved | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | | Rev 1: revised the FC value from 0x80 to 0x83 | | | | | | | | |

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of Changes\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

A.23 KIAB generation function

This input string is used when the IAB-node and the IAB-donor derive KIAB (PSK) for establishment of secure F1 interface. The following parameters shall be used to form the input S to the KDF:

- FC = 0x83,

- P0 = IAB-donor-CU IP address,

- L0 = length of IAB-donor-CU IP address,

- P1 = IAB-node DU IP address,

- L1 = length of IAB-node DU IP address.

The input key KEY shall be KgNB, if the key KgNB is in possession of the IAB-UE functionality in the IAB-node and in the IAB-donor-CU, after the IAB-UE setup procedure (Phase-1).

The input key KEY shall be S-KgNB, if the key S-KgNB is in possession of the IAB-UE functionality in the IAB-node and in the IAB-donor-CU, after dual connectivity procedure.

The entire output of the KDF (256 bits) is used as the KIAB.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of Changes\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*