**3GPP TSG-SA3 Meeting #103-e *S3-211645***

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

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.501** | **CR** | **1090** | **rev** |  | **Current version:** | **17.1.0** |  |
|  | | | | | | | | |
| *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 |  | ME |  | Radio Access Network |  | Core Network |  |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Assign FC Value for KTIPSec and KTNAP Derivation in R17 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Huawei, HiSilicon | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | 5WWC | | | | |  | ***Date:*** | | | 2021-05-10 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | A |  | | | | | ***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:*** | | In Annex A.22 in TS 33.501, there is no FC value for derivation of KTIPSec and KTNAP.  An EN is added “Editor's Note: The FC value needs to be specified.” | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Delete the EN and allocate new FC value.  This is mirror contribution. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Specification is not complete. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | Annex A.22 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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 1st Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

# A.22 KTIPSec and KTNAP derivation function

When deriving a KTIPSec from KTNGF and when deriving a KTNAP from KTNGF the following parameters shall be used to form the input S to the KDF.

- FC = 0x84

- P0 = Usage type distinguisher

- L0 = length of Usage type distinguisher (i.e. 0x00 0x01)

The values for the Usage type distinguisher are defined in table A.22-1. The values 0x00 and 0x03 to 0xf0 are reserved for future use, and the values 0xf1 to 0xff are reserved for private use.

The Usage type distinguisher shall be set to the value for IPSec (0x01) when deriving KTIPSec. The Usage type distinguisher shall be set to the value for TNAP (0x02) when deriving KTNAP.

The input key KEY shall be the 256-bit KTNGF or KTWIF.

Table A.22-1: Usage type distinguishers

|  |  |
| --- | --- |
| Usage type distinguisher | Value |
| IPSec | 0x01 |
| TNAP | 0x02 |

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

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

## A.1.2 FC value allocations

The FC number space used is controlled by TS 33.220 [28], FC values allocated for the present document are in range of 0x69 – 0x79, 0x7B – 0x7D and 0x83-0x84.

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