**3GPP TSG-CT WG6 Meeting #91 *C6-180623***

**West Palm Beach (USA), 27th November – 30th November 2018**

|  |
| --- |
| *CR-Form-v11.1* |
| **CHANGE REQUEST** |
|  |
|  | **31.102** | **CR** | **0820** | **rev** | **-** | **Current version:** | **15.2.0** |  |
|  |
| *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:***  | Support storage of EPS NAS security algos received in 5G for mobility over N26 |
|  |  |
| ***Source to WG:*** | Qualcomm Incorporated |
| ***Source to TSG:*** | C6 |
|  |  |
| ***Work item code:*** | 5GS\_Ph1-CT |  | ***Date:*** | 2018-11-19 |
|  |  |  |  |  |
| ***Category:*** | **C** |  | ***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:*** | 3GPP TS 33.501 clause 6.7.2 specifies the following:*In case the network supports interworking using the N26 interface between MME and AMF, the AMF shall also include the selected EPS NAS algorithms (defined in Annex B of TS 33.401 [10]) to be used after mobility to EPS in the NAS Security Mode Command message (see clause 8.5.2).* ***The UE shall store the algorithms for use after mobility to EPS using the N26 interface between MME and AMF****.*Additionally, S3-183619 clause 8.4.2 agreed in SA#93 specifies the following:***The UE shall further set the selected EPS NAS security algorithms in the 5G security context*** *to the NAS security algorithms used with the source MME.*This applies both when the UE access is via 3gpp and non-3gpp access. Based on the above text from TS 33.501, the EPS NAS security algorithms received in 5G NAS SMC should also be stored as part 5G NAS security context parameters in the USIM to support plastic roaming. |
|  |  |
| ***Summary of change:*** | As EPS NAS security algos received by the UE from the AMF when in 5G is specified to be a part of 5G NAS security context, enhance the existing EF5GS3GPPNSC and EF5GSN3GPPNSC files to also store the EPS NAS security algos to be used during mobility from 5G to EPS, when interworking over N26 interface and the UE supports S1 mode. |
|  |  |
| ***Consequences if not approved:*** | It is beneficial to store the EPS security algos received in 5G NAS SMC, for a later use by the UE when moving from 5G to EPS, for example, or when the USIM is inserted in another UE the new UE can use them as well, for mobility from 5G to EPS. |
|  |  |
| ***Clauses affected:*** | 4.4.11.4, 4.4.11.5, Annex D |
|  |  |
|  | **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:*** |  |

#### 4.4.11.4 EF5GS3GPPNSC (5GS 3GPP Access NAS Security Context)

If service n°122 is "available" in EFUST, this file shall be present.

This EF contains the 5GS 3GPP access NAS security context as defined in TS 24.501 [104], consisting of KAMF with the associated key set identifier, the UE security capabilities, and the uplink and downlink NAS COUNT values. This EF also contains the EPS NAS security algorithms to be used when the UE goes to EPS, either by means of connected mode handover in a network that supports N26 interface, or by the means of idle mode mobility performed by the UE from 5GS to EPS, as specified in TS 33.501 [105]. This file shall contain one record.

|  |  |  |
| --- | --- | --- |
| Identifier: '4F03' | Structure: linear fixed | Optional |
| SFI: '03' |  |
| Record size: X bytes (X≥54) | Update activity: high |
| Access Conditions: READ PIN UPDATE PIN DEACTIVATE ADM ACTIVATE ADM |
| Bytes | Description | M/O | Length |
| 1 to X | 5GS NAS Security Context TLV Object | M | X bytes |

5GS NAS Security Context tags

|  |  |
| --- | --- |
| Description | Tag Value |
| 5GS NAS Security Context Tag | 'A0' |

5GS NAS Security Context information

|  |  |  |  |
| --- | --- | --- | --- |
| Description | Value | M/O | Length (bytes) |
| 5GS NAS Security Context Tag | 'A0' | M | 1 |
| Length (length of all subsequent data) | Y | M | Note 1 |
| ngKSITag | '80' | M | 1 |
| Length | K | M | Note 1 |
| ngKSI | -- | M | K |
| KAMF Tag | '81' | M | 1 |
| Length | L | M | Note 1 |
| KAMF | -- | M | L |
| Uplink NAS count Tag | '82' | M | 1 |
| Length | M | M | Note 1 |
| Uplink NAS count | -- | M | M |
| Downlink NAS count Tag | '83' | M | 1 |
| Length | N | M | Note 1 |
| Downlink NAS count  | -- | M | N |
| Identifiers of selected NAS integrity and encryption algorithms Tag | '84' | M | 1 |
| Length | S | M | Note 1 |
| Identifiers of selected NAS integrity and encryption algorithms | -- | M | S |
| Identifiers of selected EPS NAS integrity and encryption algorithms for use after mobility to EPS Tag | '85' | M | 1 |
| Length | U | M | Note 1 |
| Identifiers of selected EPS NAS integrity and encryption algorithms for use after mobility to EPS | -- | M | U |
| Note 1: The length is coded according to ISO/IEC 8825-1 [35] |

- ngKSITag '80'

Contents:

The ngKSI (Key Set Identifier in 5G) as defined in TS 33.501 [105] is coded on 1 byte.

Coding:

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | b8 | b7 | b6 | b5 | b4 | b3 | b2 | b1 |
|  |  |  |  |  |  |  |  |  |  | ngKSI |
|  |  |  |  |  |  |  |  |  |  | bits b4 to b8 are coded 0 |

- KAMF Tag '81'

Contents:

The KAMF as defined in TS 33.501 [105] is coded on 32 bytes. The ME shall treat any KAMF values stored in this EF as invalid if the ngKSI indicates that no KAMF is available or if the length indicated in the KAMF TLV is set to '00',

Coding:

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

- Uplink NAS count Tag '82'

Contents:

The uplink NAS count as defined in TS 33.501 [105] is coded on 4 bytes.

Coding:

The most significant bit of the uplink NAS count is the most significant bit of the 1st byte of this TLV value field. The least significant bit of the uplink NAS count is the least significant bit of the last byte of this TLV value field.

- Downlink NAS count Tag '83'

Contents:

The downlink NAS count as defined in TS 33.501 [105] is coded on 4 bytes.

Coding:

The most significant bit of the downlink NAS count is the most significant bit of the 1st byte of this TLV value field. The least significant bit of the downlink NAS count is the least significant bit of the last byte of this TLV value field.

- Identifiers of selected NAS integrity and encryption algorithms Tag '84'

Contents:

The identifiers of selected NAS integrity and encryption algorithms as defined in TS 33.501 [105] and TS 24.501 [104]. In this release the identifiers of selected NAS integrity and encryption algorithms are coded as 4-bit identifiers.

Coding:

Coding is same as the content of the NAS security algorithms information element defined in TS 24.501 [104].

Byte 1 of this TLV value field: first byte of the value part of the NAS security algorithms information element

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | b8 | b7 | b6 | b5 | b4 | b3 | b2 | b1 |
|  |  |  |  |  |  |  |  |  |  |
|  |  | MSB |  |  |  |  |  |  |  |

* Identifiers of selected EPS NAS algorithms for use after mobility to EPS Tag '85'

Contents:

The identifiers of selected EPS NAS integrity and encryption algorithms to be used when the UE goes to EPS, either by means of connected mode handover in a network that supports N26 interface, or by the means of idle mode mobility performed by the UE from 5GS to EPS, as specified in TS 33.501 [105] and TS 24.501 [104]. These identifiers are coded as 4-bit identifiers.

Coding:

Coding is same as the content of the EPS NAS security algorithms information element specified in TS 24.301 [51].

Byte 1 of this TLV value field: first byte of the value part of the EPS NAS security algorithms information element in TS 24.301 [51].

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | b8 | b7 | b6 | b5 | b4 | b3 | b2 | b1 |
|  |  |  |  |  |  |  |  |  |  |
|  |  | MSB |  |  |  |  |  |  |  |

Unused bytes shall be set to 'FF'.

In order to mark the stored 5GS NAS security context as invalid:

- the record bytes shall be set to 'FF', or

- the ngKSI is set to '07', or

- the length indicated in the KAMF TLV is set to '00'.

#### 4.4.11.5 EF5GSN3GPPNSC (5GS non-3GPP Access NAS Security Context)

If Service n°122 is "available" in EFUST, this file shall be present.

This EF contains the 5GS non-3GPP access NAS security context as defined in TS 24.501 [104], consisting of KAMF with the associated key set identifier, the UE security capabilities, and the uplink and downlink NAS COUNT values. This EF also contains the EPS NAS security algorithms to be used when the UE goes to EPS, either by means of connected mode handover in a network that supports N26 interface, or by the means of idle mode mobility performed by the UE from 5GS to EPS, as specified in TS 33.501 [105]. This file shall contain one record.

|  |  |  |
| --- | --- | --- |
| Identifier: '4F04' | Structure: linear fixed | Optional |
| SFI: '04' |  |
| Record size: X bytes (X≥54) | Update activity: high |
| Access Conditions: READ PIN UPDATE PIN DEACTIVATE ADM ACTIVATE ADM |
| Bytes | Description | M/O | Length |
| 1 to X | 5GS NAS Security Context TLV Object | M | X bytes |

For content and coding see clause 4.4.11.4 for EF5GS3GPPNSC.

\*\*\*\*\* Next change \*\*\*\*\*

Annex D (informative):
Tags defined in 31.102

|  |  |  |
| --- | --- | --- |
| Tag | Name of Data Element | Usage |
| '43' | Full name for network IEI | PLMN Network Name (EFPNN) |
| '45' | Short name for network IEI | PLMN Network Name (EFPNN) |
| … | … | … |
| 'A0' | EARFCN List tagThe following tags are encapsulated within 'A0' '80' EARFCN tag '81' Geographical Area – Polygon tag | EARFCN list for MTC/NB-IOT UEs (EFEARFCNList) |
| 'A0' | 5GS 3GPP access NAS security Context tag or 5GS non-3GPP access NAS security Context tagThe following tags are encapsulated within 'A0''80' ngKSITag'81' KAMF Tag'82' Uplink NAS count Tag'83' Downlink NAS count Tag'84' Identifiers of selected NAS integrity and encryption algorithms Tag'85' Identifiers of selected EPS NAS integrity and encryption algorithms for use after mobility to EPS Tag | 5GS 3GPP Access NAS Security Context (EF5GS3GPPSNSC) or 5GS non-3GPP Access NAS Security Context (EF5GSN3GPPSNSC) |
| … | … | … |
| 'DD' | GBA Security Context Bootstrapping Mode tag | AUTHENTICATE command parameter, in GBA security context |
| 'DE' | GBA Security Context NAF Derivation Mode tag | Response to AUTHENTICATE |

NOTE: the value 'FF' is an invalid tag value. For ASN.1 tag assignment rules see ISO/IEC 8825-1 [35]