**3GPP TSG-SA3 Meeting #101-e *S3-20aabb***

**e-meeting, 9th - 20th November 2020 was S3-202947**

|  |
| --- |
| *CR-Form-v12.0* |
| **CHANGE REQUEST** |
|  |
|  | **33.501** | **CR** | **0962** | **rev** | **1** | **Current version:** | **16.4.0** |  |
|  |
| *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 |  | Core Network | **x** |

|  |
| --- |
|  |
| ***Title:***  | Correct NAS uplink COUNT for KgNB/KeNB derivation |
|  |  |
| ***Source to WG:*** | MediaTek Inc. |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | TEI16 |  | ***Date:*** | 2020-11-18 |
|  |  |  |  |  |
| ***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 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:*** | Discussion paper in S3-20aabb "NAS uplink COUNT used for AS SMC at radio bearer establishment".Need to be clarified what is the correct NAS uplink COUNT value to be used as a freshness parameter in the derivation of the KgNB/KeNB when the AS SMC is received without corresponding NAS SMC. |
|  |  |
| ***Summary of change:*** | NAS uplink COUNT of the NAS uplink message that triggered transmission from IDLE to CONNECTED mode is used as a refreshness parameter. |
|  |  |
| ***Consequences if not approved:*** | If prior to an AS SMC is received the UE has sent more than one NAS uplink message, it's unclear what is the message and corresponding NAS uplink COUNT to be used as a freshness parameter in the derivation of the KgNB/KeNB. |
|  |  |
| ***Clauses affected:*** | 6.8.1.2.2 |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** |  |  |  Other core specifications  | TS/TR ... CR ...  |
| ***affected:*** |  |  |  Test specifications | TS/TR ... CR ...  |
| ***(show related CRs)*** |  |  |  O&M Specifications | TS/TR ... CR ...  |
|  |  |
| ***Other comments:*** |  |
|  |  |
| ***This CR's revision history:*** |  |

##### 6.8.1.2.2 Establishment of keys for cryptographically protected radio bearers in 3GPP access

This sub-clause applies to establishment of keys for cryptographically protected radio bearers in 3GPP access only.

The procedure the UE uses to establish cryptographic protection for radio bearers is initiated by an NAS Service Request message or Registration Request message with "PDU session(s) to be re-activated" included from the UE to the AMF. The AMF may initiate the procedure to establish cryptographic protection for radio bearers when "PDU session(s) to be re-activated" is not included in the Registration request and but there is pending downlink UP data or pending downlink signalling.

Upon receipt of the NAS message, if the AMF does not require a NAS SMC procedure before initiating the NGAP procedure INITIAL CONTEXT SETUP, the AMF shall derive key KgNB/KeNB as specified in Annex A using the uplink NAS COUNT (see TS 24.501 [35]) corresponding to the NAS message that initiated transition from CM-IDLE to CM-CONNECTED state and the KAMF of the current 5G NAS security context.

The AMF shall communicate the KgNB/KeNB to the serving gNB/ng-eNB in the NGAP procedure INITIAL CONTEXT SETUP. The UE shall derive the KgNB/KeNB from the KAMF of the current 5G NAS security context using the NAS uplink COUNT corresponding to the NAS message that initiated transition from CM-IDLE to CM-CONNECTED state.

As a result of the NAS Service Request or Registration procedure, with "PDU session(s) to be re-activated" radio bearers are established, and the gNB/ng-eNB sends an AS SMC to the UE. When the UE receives the AS SMC without having received a NAS Security Mode Command, it shall use the NAS uplink COUNT corresponding to the that initiated transition from CM-IDLE to CM-CONNECTED state as freshness parameter in the derivation of the KgNB/KeNB. The KDF as specified in Annex A shall be used for the KgNB/KeNB derivation using the KAMF of the current 5G NAS security context. From the KgNB/KeNB the RRC protection keys and the UP protection keys are derived by the UE and the gNB/ng-eNB as described in sub-clause 6.2.

If the NAS procedure establishing radio bearers contains a primary authentication run (which is optional), the NAS uplink and downlink COUNT for the new KAMF shall be set to the start values (i.e. zero). If the NAS procedure establishing radio bearers contains a NAS SMC (which is optional), the value of the uplink NAS COUNT corresponding to the most recent NAS Security Mode Complete shall be used as freshness parameter in the KgNB/KeNB derivation from fresh KAMF of the current 5G NAS security context when executing an AS SMC. The KDF as specified in Annex A shall be used for the KgNB/KeNB derivation also in this case.