**3GPP TSG-SA3 Meeting #106-e *S3-220502***

**e-meeting, 14 - 25 February 2022 revision of *S3-220423***

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.501** | **CR** | 1356 | **rev** | **-** | **Current version:** | **17.4.2** |  |
|  | | | | | | | | |
| *For* ***[HE](http://www.3gpp.org/3G_Specs/CRs.htm" \l "_blank)******LP*** *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 | **X** | Core Network |  |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Remove ambiguous phrase for rekeying error scenario in clause 6.9.2.3.2. | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | NTT DOCOMO, Nokia, Nokia Shanghai Bell | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | 5GS\_Ph1-SEC, TEI17 | | | | |  | ***Date:*** | | | 2022-02-01 |
|  |  | | | |  | |  | | |  |
| ***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-15 (Release 15) Rel-16 (Release 16) Rel-17 (Release 17) Rel-18 (Release 18)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | According to the proposal in S3-201078, some AS level rekeying failure scenarios need response from gNB to AMF, and some failure scenarios do not need this response. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | This is a very rare error scenario and SA3 need not change AMF behaviour for this. Hence, it is proposed to remove the ambiguous phrase “and send appropriate response to AMF” in clause 6.9.2.3.2. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Ambiguous phrase for rekeying error scenario remains. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 6.9.2.3.2 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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 the Change---

6.9.2.3.2 Xn-handover

In Xn handovers the source gNB/ng-eNB shall perform a vertical key derivation in case it has an unused {NH, NCC} pair. The source gNB/ng-eNB shall first compute KNG-RAN\* from target PCI, its frequency ARFCN-DL/EARFCN-DL, and either from currently active KgNB in case of horizontal key derivation or from the NH in case of vertical key derivation as described in Annex A.11/A.12.

Next, the source gNB/ng-eNB shall forward the { KNG-RAN\*, NCC} pair to the target gNB/ng-eNB. The target gNB/ng-eNB shall use the received KNG-RAN\* directly as KgNB to be used with the UE. The target gNB/ng-eNB shall associate the NCC value received from source gNB/ng-eNB with the KgNB. The target gNB/ng-eNB shall include the received NCC into the prepared HO Command message, which is sent back to the source gNB/ng-eNB in a transparent container and forwarded to the UE by source gNB/ng-eNB.

When the target gNB/ng-eNB has completed the handover signalling with the UE, it shall send a NGAP PATH SWITCH REQUEST message to the AMF. Upon reception of the NGAP PATH SWITCH REQUEST, the AMF shall increase its locally kept NCC value by one and compute a new fresh NH from its stored data using the function defined in Annex A.10. The AMF shall use the KAMF from the currently active 5G NAS security context for the computation of the new fresh NH. The AMF shall then send the newly computed {NH, NCC} pair to the target gNB/ng-eNB in the NGAP PATH SWITCH REQUEST ACKNOWLEDGE message. The target gNB/ng-eNB shall store the received {NH, NCC} pair for further handovers and remove other existing unused stored {NH, NCC} pairs if any.

If the AMF had activated a new 5G NAS security context with a new KAMF, different from the 5G NAS security context on which the currently active 5G AS security context is based, but has not yet successfully performed a UE Context Modification procedure, the sent NGAP PATH SWITCH REQUEST ACKNOWLEDGE message shall in addition contain a NSCI (New Security Context Indicator). The AMF shall in this case derive a new initial KgNB from the new KAMF and the uplink NAS COUNT in the most recent NAS Security Mode Complete message as specified in Annex A.9. The AMF shall associate the derived new initial KgNB with a new NCC value equal to zero. Then, the AMF shall use {the derived new initial KgNB, the new NCC value initialized to zero} pair as the newly computed {NH, NCC} pair to be sent in the NGAP PATH SWITCH REQUEST ACKNOWLEDGE message. The gNB/ng-eNB shall in this case set the value of *keySetChangeIndicator* field to true in further handovers. The gNB/ng-eNB should in this case perform an intra-gNB-CU/intra-ng-eNB handover immediately .

NOTE 1: Because the NGAP PATH SWITCH REQUEST message is transmitted after the radio link handover, it can only be used to provide keying material for the next handover procedure. Thus, for Xn-handovers key separation happens only after two hops because the source gNB/ng-eNB knows the target gNB/ng-eNB keys. The target gNB/ng-eNB can immediately initiate an intra-gNB-CU/intra-ng-eNB handover to take the new NH into use once the new NH has arrived in the PATH SWITCH REQUEST ACKNOWLEDGE message.

NOTE 2: The key derivation mechanism described in this clause is also applicable to CHO defined in TS 38.300[52].

---End of the Change---