**3GPP TSG-SA3 Meeting #124 draft\_S3-253668-r2**

**Wuhan, China, 13 – 17 October 2025**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **33.501** | **CR** | **2188** | **rev** | **1** | **Current version:** | **19.4.0** |  |
|  |
| *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 | **X** | Core Network |  |

|  |
| --- |
|  |
| ***Title:***  | Update to security handling when CU is acting as MN and SN is unchanged |
|  |  |
| ***Source to WG:*** | Xiaomi, Huawei, HiSilicon |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | NR\_Mob\_Ph4\_Sec |  | ***Date:*** | 2025-10-06 |
|  |  |  |  |  |
| ***Category:*** | F |  | ***Release:*** | Rel-19 |
|  | *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-15 (Release 15)Rel-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)* |
|  |  |
| ***Reason for change:*** | As agreed in R3-256004, LTM information from source gNBs is transferred with HANDOVER REQUEST message. If security capability mismatches, the gNB will update AS security context with security capability.Term alignment with R3-256003.Security mechanism and procedures for L1/L2 triggered mobility with DC configuration is specified in clause 6.17.2 of TS 33.501. It is specified that the MN shall assign a sequence of distinct SN Counter values (maintained for dual connectivity detailed in clause 6.10.3.1 of this document) per candidate gNB to UE. However, such specification is not align with RAN2 decision. According to R2-2504702, it was concluded (for RRC-7) that the legacy sk-counter is used for inter-MN LTM (this means sk-counter value can be re-used). This conclusion resolved the editor’s note for RRC-7 on whether the list of sk-counters can be used only for the case of inter-MN LTM. In addition, it was agreed at RAN2#131 that the UE shall not perform secondary key change when intra-MN LTM is performed.Given the above agreements reached by RAN2, there is no need to assign a sequence of distinct SN counter values for DC to the UE. The UE can reuse the SN counter value configured by the MN during the preparation phase to derive the KSN. Once there is an inter-MN LTM, the KSN can be updated using the same SN coutner value as the KgNB is updated. Once there is an intra-MN LTM, there is no need to update the KSN according to RAN2 agreement. |
|  |  |
| ***Summary of change:*** | 1. Added detailed message in preparation phase.
2. Added clarification to the security capability mismatch case.
3. Revised the use case term.

Removed the sepcification not aligned with RAN2 agreements. |
|  |  |
| ***Consequences if not approved:*** | Potential ambiguity in stage 2 specificationMisalignment between RAN2 and SA3 |
|  |  |
| ***Clauses affected:*** | 6.17.1, 6.17.2 |
|  |  |
|  | **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:*** |  |

\* \* \* First Change \* \* \* \*

## 6.17 Security mechanism and procedures for L1/L2 Triggered Mobility

### 6.17.1 When DC is not configured

For the case where CU is acting as MN and DC is not configured as specified in TS 38.300 [52], during LTM preparation phase, the serving gNB shall send the {KNG-RAN\*, NCC} pair (per candidate cell), UE's 5G security capabilities, ciphering and integrity algorithms used in the serving cell and the UE's UP security policy along with the UE security context with HANDOVER REQUEST message to the candidate gNB(s). The candidate gNB(s) shall send the LTM configuration(s) (containing the selected AS security algorithms and the UE’s UP security activation status) with HANDOVER REQUEST ACKNOWLEDGE message to the serving gNB for the accepted candidate cell(s). The serving gNB shall send the RRCReconfiguration message to the UE including the LTM candidate configurations containing the selected AS security algorithms and the UE’s UP security activation status.

The {KNG-RAN\*, NCC} pair at the candidate cells shall require updating when there is a newly derived key KgNB or unused pair of {NCC, NH} at the serving gNB, e.g. due to an inter-CU handover/cell switch or an intra-CU handover/cell switch with a change of key. To update the candidate cells, the serving gNB shall generate the KNG-RAN\* as described in Annex A.11 and send the generated {KNG-RAN\*, NCC} pair (per candidate cell) to the candidate gNB(s) using LTM Configuration Update message.

During LTM execution phase, the serving gNB includes the NCC used for the derivation of KNG-RAN\* in the *Cell Switch Command MAC CE* to the UE. Upon receiving the cell switch command, the UE derives the KNG-RAN\* as described in clause 6.9.2.3.4 of the present document and switches to the target gNB.

NOTE: Key changes that use the keySetChangeIndicator field to be set to true use the normal L3 handover.

If the target gNB receives NSCI (as detailed in clause 6.9.2.3.2) or UE's 5G security capabilities from the AMF (as detailed in clause 6.7.3.1 of the present document) and/or UE's UP security policy from the SMF (as detailed in clause 6.6.1 of the present document) in the Path-Switch Acknowledge message, then the target gNB may update the 5G security capabilities and initiate an intra-gNB-CU handover to refresh KNG-RAN\* or activate or de-activate the UP integrity/confidentiality as per the received policy from SMF or to indicate the selected algorithms appropriately. Further, the target gNB either releases the LTM configuration (UE's 5G security capabilities and/or UE's UP security policy) or updates the LTM configuration (e.g., delete the LTM context and reinitiated LTM preparation) to the candidate cells. If necessary, the serving gNB then updates the UE with the configuration (i.e., the selected AS security algorithms and/or the UE’s UP security activation status) aligned with LTM configuration in the network.

### 6.17.2 When DC is configured

In case of inter-SN SCG LTM as specified in TS 37.340 [51], the security mechanism and procedures as specified in clause 6.10.2.4 of this specification for SCPAC shall be applied.

In case of inter-MN MCG LTM with SN as specified in TS 37.340 [51], MN follows the same procedure as specified in the non-DC case. Upon receiving the MAC CE message with NCC, the UE shall derive the SN keys with the existing SN counter. The UE sends the RRC Reconfiguration Complete to the MN. The UE shall activate the chosen encryption/decryption and integrity protection keys with the SN at this point. In the network side, the MN shall deliver the KSN to SN when KgNB is available. If the KSN is not received in SN and SN received uplink messages, the SN shall defer the messages until the security activation. SN activates the chosen encryption/decryption and integrity protection with UE on receipt of SN Reconfiguration Complete message or upon receiving the Random-Access request from the UE.

\* \* \* End of Change \* \* \* \*