3GPP TSG-SA3 Meeting #123 draft\_S3-252948-r1

Goteborg, Sweden, 25 – 29 August 2025

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  |  | **CR** | **2170** | **rev** | **1** | **Current version:** |  |  |
|  | | | | | | | | |
| *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 | **X** | Core Network |  |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Correction to security mechanism and procedures for L1/L2 Triggered Mobility | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Samsung | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** |  | | | | |  | ***Date:*** | | | 2025-08-11 |
|  |  | | | |  | |  | | |  |
| ***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 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:*** | | The following paragraph from clause 6.17.1 seems incomplete:  “The {KNG-RAN\*, NCC} pair at the candidate cells require updating when a new key 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 send the generated {KNG-RAN\*, NCC} pair (per candidate cell) to the candidate gNB(s) using LTM Configuration Update message” | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | To be updated as follows:  “The {KNG-RAN\*, NCC} pair at the candidate cells shall require updating when there is a newly derived key KgNB and/or an 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.” | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Incomplete specification leads to ambiguity. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 6.17.1 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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 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) 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 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 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 or updates the LTM configuration (UE's 5G security capabilities and/or UE's UP security policy) of the candidate cells. If necessary, the serving gNB then updates the UE with the configuration aligned with LTM configuration in the network.

\* \* \* End of Changes \* \* \* \*