**3GPP TSG-SA3 Meeting #105-e *S3-214138r1***

**e-meeting, 8 - 19 November 2021** *revision of S3-214138*

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **33.401** | **CR** | **0700** | **rev** | **1** | **Current version:** | **16.3.0** |  |
|  |
| *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 |  | Radio Access Network | **X** | Core Network | **X** |

|  |
| --- |
|  |
| ***Title:***  | Confirming UE supported algorithms in Path Switch procedure |
|  |  |
| ***Source to WG:*** | Qualcomm Incorporated |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | TEI17 |  | ***Date:*** | 2021-10-28 |
|  |  |  |  |  |
| ***Category:*** | C |  | ***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 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:*** | Unlike with the 5G Core and the EPS handling of the NR UE Security Capabilities (clause E.3.4.3 of TS 33.401), EPS does not provide the eNB with an update (in the path switch procedure) of the (LTE) UE security capabilities if a mis-match is detected by the MME.This is a disadvantage for the future introduction of LTE algorithms. |
|  |  |
| ***Summary of change:*** | The MME shall return its locally stored UE EPS security capabilities to the target eNB in the response to the path-switch message if the eNB had the incorrect set of algorithms. The eNB then performs an algorithm selection based on the returned UE EPS security capabilities to the target eNB and performs an intra-cell handover to change the in-use algorithms if these are different to the selected ones. |
|  |  |
| ***Consequences if not approved:*** |  |
|  |  |
| ***Clauses affected:*** | 7.2.4.2.2 |
|  |  |
|  | **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:*** | Rev 1 updates the eNB behaviour on discovering different algorithms currently in use and add more details to reason for change. |

**\*\*\*\* START OF CHANGES \*\*\*\***

7.2.4.2.2 X2-handover

At handover from a source eNB over X2 to a target eNB, the source eNB shall include the UE EPS security capabilities and ciphering and integrity algorithms used in the source cell in the handover request message. The target eNB shall select the algorithm with highest priority from the UE EPS security capabilities according to the prioritized locally configured list of algorithms (this applies for both integrity and ciphering algorithms). The chosen algorithms shall be indicated to the UE in the handover command if the target eNB selects different algorithms compared to the source eNB. If the UE does not receive any selection of integrity and ciphering algorithms it continues to use the same algorithms as before the handover (see TS 36.331 [21]). In the path-switch message, the target eNB shall send the UE EPS security capabilities received from the source eNB to the MME. The MME shall verify that the UE EPS security capabilities received from the eNB are the same as the UE EPS security capabilities that the MME has stored. If there is a mismatch, the MME shall send its locally stored UE EPS security capabilities to the target eNB in the response to the path-switch message. In addition, the MME may log the event and may take additional measures, such as raising an alarm. If the target eNB receives UE EPS security capabilities from the MME, the target eNB shall update the AS security context of the UE with these UE EPS security capabilities. The target eNB shall select the algorithm with highest priority from these UE EPS security capabilities according to the locally configured prioritized list of algorithms (this applies for both integrity and ciphering algorithms). If the algorithms selected by the eNB are different from the algorithms currently used at the target eNB, then the target eNB may take the proper actions to change to the selected algorithms.

NOTE: Transferring the ciphering and integrity algorithms used in the source cell to the target eNB in the handover request message is for the target eNB to decipher and integrity verify the RRCReestablishmentComplete message on SRB1 in the potential RRCConnectionRe-establishment procedure. The information is also used by the target eNB to decide if it is necessary to include a new selection of security algorithms in the handover command.

**\*\*\*\* END OF CHANGES \*\*\*\***