**3GPP TSG-SA3 Meeting #121 S3-251743**

**Goteborg, Sweden, 7 – 11 April 2025**

|  |
| --- |
| *CR-Form-v12.1* |
| **Draft CHANGE REQUEST** |
|  |
|  | **33.401** | **CR** |  **draft** | **rev** |  | **Current version:** | **18.3.0** |  |
|  |
| *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 |  | Core Network | **x** |

|  |
| --- |
|  |
| ***Title:***  | Living document for security aspects of 5G satellite access phase 3 |
|  |  |
| ***Source to WG:*** | CATT |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | 5GSAT\_Ph3\_SEC |  | ***Date:*** | 2025-04-07 |
|  |  |  |  |  |
| ***Category:*** | **B**  |  | ***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:*** | Security for 5G satellite access phase 3 is not specified yet. |
|  |  |
| ***Summary of change:*** | Provide specification for security aspects of 5G satellite access phase 3 in a new normative annex in TS 33.401. |
|  |  |
| ***Consequences if not approved:*** | Specification is not complete. |
|  |  |
| ***Clauses affected:*** | Annex X (new) |
|  |  |
|  | **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 1st Change \*\*\*

Annex X (normative):
Security for Store and Forward Satellite operation

# X.1 General

This Annex describes the security aspects of Store and Forward Satellite operation. The general features of Store and Forward Satellite operation are described in 23.401 [2].

There are two example deployment options for Store and Forward Satellite operation given in Annex O of TS 23.401 [2], i.e. Split MME architecture and Full EPC in each satellite. In both cases, regular LTE procedures shall be used to provide the security between the UE and network, e.g. authentication and protection of traffic between the UE and network.

The security of communications between the proxies on satellite and the ground station(s) is out of 3GPP scope.

NOTE: The following informative text in clauses X.2 and X.3 outlines security aspects of the two deployment options as described in Annex O.2 and O.3 of TS 23.401 [2].

# X.2 Security aspects of Split MME architecture

Mutual authentication between the UE and the network in a split MME architecture can involve more than one satellite (i.e., more than one MME-onboard), in which case the ground segment of the network is responsible for the selection and provisioning of MME-onboard the same, or another satellite, with the necessary information (e.g., Authentication Vector) to perform or finish an authentication procedure. The MME on-board obtains the EPS authentication vectors when the feeder link is available, and stores the authentication vectors when the service link is unavailable.

The NAS security shall be terminated on the MME-onboard. The ground segment of the network shall ensure that the latest NAS security context of the UE, or an Authentication Vector, is available at the MME-onboard.

NOTE: The distribution and synchronization of the latest NAS security context between the MME-ground and MME-onboard is out of the scope of 3GPP.

# Editor’s Note: Addressing (D)DOS attack is FFS.X.3 Security aspects of Full EPC in each satellite

The security credentials required for the mutual authentication are stored in the HSS onboard the satellite. To enable having only a satellite-specific subscriber key stored in the satellite, IOPS-based keying method described in Annex F of the present document is used to limit the impact of exposing long-term keys in the HSS onboard the satellite.

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