**33GPP TSG-SA3 Meeting #123 draft\_S3-252936-r1**

Goteborg, Sweden, 25 – 29 August 2025revision of S3-252842

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **33.401** | **CR** |  | **rev** | **-** | **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 | **X** |

|  |
| --- |
|  |
| ***Title:***  |  |
|  |  |
| ***Source to WG:*** | Thales |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** |  5GSAT\_Ph3\_SEC |  | ***Date:*** | 2025-08-14 |
|  |  |  |  |  |
| ***Category:*** |  |  | ***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:*** | In NOTE 2, low processing and storage capabilities on board satellites seems to apply to all types of satellites, while in reality this may apply only to some types of satellites.  |
|  |  |
| ***Summary of change:*** | The description of low processing and storage capabilies on board satellites is modified not to be generic, and not to apply to all types of satellites.  |
|  |  |
| ***Consequences if not approved:*** | The current description is misleading since it suggests that the low processings and storage capabilities on board satellites applies to all satellites, which is not correct.  |
|  |  |
| ***Clauses affected:*** | N.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:*** |  |

# N.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.

According to clause 4.13.9.1 of TS 23.401 [2] the MME rejects a NAS procedure if the MME-onboard cannot complete the NAS procedure with the information it has available. Hence the NAS security is terminated on the MME-onboard, and the ground segment of the network ensures that the latest NAS security context of the UE, or an Authentication Vector, is available at the MME-onboard.

NOTE 1: The distribution and synchronization of the latest NAS security context between the MME-ground and MME-onboard is out of the scope of 3GPP.

NOTE 2: The security environment is likely to have to accommodate lower processing and storage capabilities on board the satellite compared to terrestrial communication equipment. Due to the feeder link temporary unavailability in split-MME deployment, a malicious entity can flood satellites with spoofed Attach Requests (unauthenticated Attach Requests). This consumes storage space in the MME-onboard before authentication occurs, hence potentially resulting in (D)DoS attack on the Satellite. Addressing said (D)DoS attack in the Split MME deployment is left to implementation.