**3GPP TSG-SA3 Meeting #123 Draft S3-253017**

Goteborg, Sweden, 25 – 29 August 2025

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **926** | **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 |  | Core Network |  |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Introducing the threat to AMF which was approved but not implemented in 33.926 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Huawei, HiSilicon, CAICT | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | SCAS\_5GA | | | | |  | ***Date:*** | | | 2025-08-18 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **F** |  | | | | | ***Release:*** | | | Rel-20 |
|  | *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:*** | | A new threat ‘Failure to deregister UE after NSSAA revocation’ was approved by SA3, as shown in S3-212380, but not implemented in the published 33.926. This CR is to re-propose this threat. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Introducing the threat to AMF which was approved but not implemented. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Low quality of SCAS documents. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | K.2.10 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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 threat is referred by S3-253032, please make sure the clause number are synchronized. | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | |  | | | | | | | | |

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* START of CHANGES\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

## K.2.10 Threats related to session establishment procedure

### K.2.10.1 Incorrect validation of S-NSSAIs

- *Threat name*: Incorrect Validation of S-NSSAIs.

- *Threat category*: Elevation of Privilege.

- *Threat Description*: After the successful network slice-specific authentication and authorization, there will be an Allowed NSSAI list both in UE and AMF. Then, the UE will initiate the PDU session establishment request with the requested S-NSSAIs included. If the AMF does not verify whether the received S-NSSAIs is within the Allowed NSSAI list stored at the AMF, an attacker can still include the rejected S-NSSAIs in the request and access the slice after it fails the NSSAA procedure.

*- Threatened Asset:* Mobility management data, sufficient processing capacity.

### K.2.10.2 Failure to deregister UE after NSSAA revocation

- *Threat name:* Failure to deregister UE after NSSAA revocation.

- *Threat Category:* Resource misuse.

- *Threat Description:* AAA Server can initiate slice specific authorization revocation for a S-NSSAI, and after the revocation the AMF will remove the S-NSSAI from the Allowed NSSAI list. In the case where no S-NSSAI is left in Allowed NSSAI for an access after the revocation, and no Default NSSAI can be provided to the UE in the Allowed NSSAI or a previous NSSAA failed for the Default NSSAI over this access, if AMF fails to deregister the UE from the network, the UE will have unauthorized use of network slice.

- *Threatened Asset:* Sufficient Processing Capacity.\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* END of CHANGES\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*