**3GPP TSG-SA3 Meeting #104-e *S3-212667-r1***

**e-meeting, 16 - 27 August 2021**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.926** | **CR** | Draft CR | **rev** | **1** | **Current version:** | **17.1.0** |  |
|  | | | | | | | | |
| *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:*** | Adding a new threat for NSSAAF | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Huawei, HiSilicon | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | SCAS\_5G\_NSSAAF | | | | |  | ***Date:*** | | | 2021-07-09 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **B** |  | | | | | ***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 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:*** | | TS 33.501 clause 16.4 and 16.5, i.e. AAA Server triggered Network Slice-Specific Re-authentication and Re-authorization procedure and AAA Server triggered Slice-Specific Authorization Revocation, have identified the security requirement to defend against the AAA-S impersonating attack, and have accordingly defined countermeasures.  The test case in S3-21xxxx is proposed for the above security requirement. This contribution propoes the accompanying threat. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Adding a new threat to NSSAAF | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Incomplete spec | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | Annex X.2 (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 Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

## X.2.2 Threats related to NSSAAF

### X.2.2.Y Threats related to impersonating attack by AAA-S

* *Threat name:* Threats related to impersonating attack by AAA-S
* *Threat Category*: Denial of service, spoofing identity
* *Threat Description*: Network slice specific authentication and authorization (NSSAA) is performed between UE and AAA server (AAA-S). AAA-S may also trigger network slice-specific authorization revocation by sending a request to NSSAAF. After receiving the request to revoke the slice-specific authorization for a slice for a UE from an AAA-S, if NSSAAF does not check whether the AAA-S is legitimate in the sense that it had performed the NSSAA for the slice for the UE, a malicious AAA-S may masquerade as the legitimate AAA-S to invoke the slice-specific authorization for the slice for the UE. Then UE is denied access to the slice. Similarly a malicious AAA-S may also trick NSSAAF to perform slice specific re-authentication and re-authorization just to incur extra signalling load.
* *Threatened Asset*: user data related to NSSAA, processing capacity

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