**3GPP TSG-SA3 Meeting #123 S3-253016**

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:***  | Iiving document for TR 33.926 |
|  |  |
| ***Source to WG:*** | Huawei, HiSilicon, MITRE-FFRDC, US National Security Agency, CAICT |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | SCAS\_5GA |  | ***Date:*** | 2025-08-18 |
|  |  |  |  |  |
| ***Category:*** | **B** |  | ***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 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:*** | S3-252580Missing the associated threat relating to two access token verification checks to be done by NF service producer in TS 33.501 clause 13.4.1.1:1. *In the direct communication case, it checks that the NF Instance ID in the subject claim within the access token matches the NF Instance ID in the subjectAltName in the NF Service Consumer's TLS client certificate.*
2. *If the CCA is present in the service request, it may verify the CCA as specified in clause 13.3.8.3 and that the subject claim (i.e., the NF Instance Id of the NF Service Consumer) in the access token matches the subject claim in the CCA.*

There is an additional threat which belongs in TR 33.926 clause 6.3.3.1 that may occur if the access token subject claims are not verified by the NF service producer. That is, if the subject claim is not verified, then *an adversary can replay the access token. This results in access to the services allowed to another NF service consumer, which leads to spoofing identity, elevation of privilege and consequently information disclosure.*S3-252775A 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:*** | S3-252580Add a threat to clause 6.3.3.1 to cover the case when the subject claims in the access token are not verified. S3-252775Introducing the threat to AMF which was approved but not implemented. |
|  |  |
| ***Consequences if not approved:*** | S3-252580The threat corresponding to failure to verify subject claims is not documented. NF service producer products are vulnerable to impersonation attacks.S3-252775Low quality of SCAS documents. |
|  |  |
| ***Clauses affected:*** | 6.3.3.1, K.2.10.2(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:*** | The merger of S3-252580, S3-252775 |

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

#### 6.3.3.1 Elevation of privilege via incorrect verification of access tokens

- *Threat name*: Incorrect Verification of Access Tokens.

- *Threat category*: Elevation of Privilege, Information Disclosure, Denial of Service, Spoofing Identity.

- *Threat Description*: there are following threats if the generic NF cannot correctly verify the access tokens:

- An access token may be tampered so that an attacker can arbitrarily access any services from any NF service providers within the same PLMN or in different PLMNs or SNPNs, which leads to elevation of privilege and consequently information disclosure.

- An access token may be tampered so that an attacker can arbitrarily access the services of any slices provided by the NF producer instances (excluded from the list of NSSAIs or the list NSI IDs) within the same PLMN or in different PLMNs or SNPNs, which leads to elevation of privilege and consequently information disclosure.

- An access token may be tampered so that an attacker can arbitrarily access the services provided by the NF producer instances outside the NF Set which it is allowed to access within the same PLMN or in different PLMNs or SNPNs, which leads to elevation of privilege and consequently information disclosure.

- An access token may be tampered so that an attacker can arbitrarily access the disallowed resources or conduct disallowed actions on the resources for the services provided by a NF service provider within the same PLMN or in different PLMNs or SNPNs, which leads to elevation of privilege and consequently information disclosure.

- An access token may be tampered so that an attacker can block service access by replacing the granted services/NF service providers with unavailable services/NF service providers, which leads to denial of service.

- An expired access token can be replayed so that an attacker can access the services which may no longer be allowed by the NF service provider, which leads to elevation of privilege and consequently information disclosure.

- An access token can be replayed by an attacker to access the services allowed to another NF service consumer, which leads to spoofing identity, and consequently information disclosure.

*- Threatened Asset:* NF API data, NF Application, Sufficient processing capacity

NOTE 1: This SNPNs authorization aspects only apply to UDMs, NRFs and AUSFs in Credentials Holders Credentials Holder using AUSF and UDM for primary authentication..

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* END of CHANGES\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* START of 1st CHANGES\*\*\*\*\*\*\*\*\*\*\*\*\*\*

### 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\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*