**3GPP TSG-SA3 Meeting #100e *S3-20xxxx***

**e-meeting, 17 - 28 August 2020 *revision of S3-201891***

|  |
| --- |
| *CR-Form-v12.0* |
| **CHANGE REQUEST** |
|  |
|  | **33.926** | **CR** | **DraftCR** | **rev** | **-** | **Current version:** | **16.3.0** |  |
|  |
| *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:***  | Threat analysis of incorrect validation of client credentials assertion  |
|  |  |
| ***Source to WG:*** | Nokia, Nokia Shanghai Bell |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | eSCAS\_5G  |  | ***Date:*** | 07-08-2020 |
|  |  |  |  |  |
| ***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 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-12 (Release 12)**Rel-13 (Release 13)Rel-14 (Release 14)Rel-15 (Release 15)Rel-16 (Release 16)* |
|  |  |
| ***Reason for change:*** | For indirect communication where NF service consumer and NF service producer/NRF cannot mutually authenticate each other, the authentication of NF service consumer towards NF service producer can only implicitly rely on authentication between NF service consumer and SCP and between SCP and NRF/NF service producer with hop-by-hop security protection. An additional authentication for indirect communication is to use a client credentials assertion signed by the NF service consumer and validated by NRF/NF service producer, as defined in TS 33.501 clause 13.3.8. Since a client credentials assertion is not sent directly to NRF/NF service producer but forwarded by one or even several SCPs, there is the risk that the assertion could possibly be swapped by one of the SCPs accidentally on the forwarding path or even be compromised to an attacker. Therefore, it is proposed to analyse the potential threats when the NF service producer/NRF receiving the client credentials seertion cannot correctly validate it. |
|  |  |
| ***Summary of change:*** | Added a new clause for analysing the potential threats related to client credentials assertion validation by NRF/NF service producer. |
|  |  |
| ***Consequences if not approved:*** | Lack of threat anslysis for the purpose of the test cases for security assurance. |
|  |  |
| ***Clauses affected:*** | 6.2, new clause 6.3.x, 6.3.x.1 |
|  |  |
|  | **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 the 1st Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

## 6.2 Generic critical assets

The generic critical assets of NF to be protected are:

- NF Application.

- NF API data (e.g. API message IEs, access tokens, client credentials assertions).

- The interfaces of NF to be protected and which are within SECAM scope:

- Service Based Interfaces.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of the 2nd Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

### 6.3.x Threats related to authentication for indirect communication

#### 6.3.x.1 Incorrect validation of client credentials assertion

- *Threat name*: Incorrect Validation of Client Credentials Assertion.

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

- *Threat Description*: for indirect communication where NF service consumer and NRF/NF service producer cannot mutually authenticate each other, the authentication of NF service consumer towards NRF/NF service producer can only implicitly rely on authentication between NF service consumer and SCP and between SCP and NRF/NF service producer with hop-by-hop security protection. An additional authentication for indirect communication is using client credentials assertion signed by NF service consumer and validated by NRF/NF service producer, as defined in TS 33.501 [3] clause 13.3.8. Since a client credentials assertion is forwarded by one or even several intermediate nodes for indirect communication, there is the risk that the assertion could possibly be swapped by one of the intermediate nodes accidentally or even be compromised to an attacker on the forwarding path. There are following threats if the generic NF (including all typers of NF service producer, NRF) receiving the assertion cannot correctly validate it:

- If the NF could not verify the integrity of the assertion, an attacker can deceive the NF by tampering the instance ID of the consumer NF, audience claim, timestamp and expiration time in the client credentials assertion. This can lead to spoofing identity, information disclosure, denial of service, elevation of privilege, etc.

- If the NF could successfully verify the integrity of the client credentials assertion but could not verify the audience claim in the assertion, an attacker can deceive the NF with an assertion detined for another NF type intercepted from the consumer NF. This can lead to spoofing identity, information disclosure, elevation of privilege.

- If the NF could successfully verify the integrity and audience claim of the client credentials assertion but could not verify the expiration time (exp) in the assertion, it can be replayed by an attack, who can abuse the use of assertion for authentication out of its lifetime. This can lead to spoofing identity, information disclosure, etc.

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

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of the Changes \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*