**3GPP TSG-SA3 Meeting #100e *S3-201612-r1***

**e-meeting, 17-28 August 2020**

|  |
| --- |
| *CR-Form-v12.0* |
| **CHANGE REQUEST** |
|  |
|  |  | **CR** | **0881** | **rev** | **1** | **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 | **x** |

|  |
| --- |
|  |
| ***Title:***  | Access token indication of NF service consumer authentication via NRF |
|  |  |
| ***Source to WG:*** | Mavenir, Nokia, Nokia Shanghai Bell |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | 5G\_eSBA |  | ***Date:*** | 2020-08-17 |
|  |  |  |  |  |
| ***Category:*** |  |  | ***Release:*** | Rel-16 |
|  | *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:*** | In TS33.501 and under clause 13.3.2.2, it reads the following:If the PLMN uses token-based authorization as specified by clause 13.4.1.2 and the PLMN’s policy mandates that the NRF authenticates the NF Service Consumer before granting an access token, the access token indicates to the NF Service Producer that the NF Service Consumer has been authenticated by the NRF.The above statement is misleading and not completely accurate.Since an attacker can possibly steal an access token and send a service request to the NF service producer using an access token which belongs to another NF service consumer, it is important to ensure that the above statement accurate and not open for insecure interpretations.This CR propose a change to ensure that this statement is accurate and does not introduce any incorrect information. |
|  |  |
| ***Summary of change:*** | Correcting the mentioned statement to ensure that TS33.501 does not introduce any inaccurate information. |
|  |  |
| ***Consequences if not approved:*** | Inaccurate statement which allows specific attacks to be valid.. |
|  |  |
| ***Clauses affected:*** | 13.3.2.2 |
|  |  |
|  | **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:*** |  |

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of Change 1 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

### 13.3.2 Authentication and authorization between network functions

………..

………...

#### 13.3.2.2 Indirect communication

In indirect communication scenarios, the NF Service Producer and NF Service Consumer shall use implicit authentication by relying on authentication between NF Service Consumer and SCP, and between SCP and NF Service Producer, provided by the transport layer protection solution, NDS/IP, or physical security.

NOTE 0: Mutual authentication between NF service consumer and NF Service producer is not achieved with hop-by-hop security.

If the PLMN uses OAuth 2.0 token-based authorization as specified by clause 13.4.1.2 and the PLMN's policy mandates that the NRF authenticates the NF Service Consumer before granting a JWT access token, then the NRF indicates to the NF Service Producer in the issued JWT access token that the NF Service Consumer identified by the NF Instance ID that is listed in the subject of the access token has been authenticated by the NRF.

If additional authentication of the NF Service Consumer is required, the NF Service Producer authenticates the NF Service Producer at the application layer using Client credentials assertion and authentication as specified in clause 13.3.8.

The NF service consumer authentication based on Client credentials assertion and authentication is optional to use, and based on operator policy.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of Change 1 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*