**3GPP TSG-SA3 Meeting #101-e *draft\_S3-202808-r2***

**e-meeting, 09 - 20 November 2020**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  |  | **CR** | **0955** | **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 | **x** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | NRF authorization during NF service consumer Access Token Get Request | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** |  | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | 5GS\_Ph1-SEC | | | | |  | ***Date:*** | | | 2020-11-09 |
|  |  | | | |  | |  | | |  |
| ***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 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-12 (Release 12)* *Rel-13 (Release 13) Rel-14 (Release 14) Rel-15 (Release 15) Rel-16 (Release 16)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | In the current TS33.501, in clause 13.4.1.1, there is misalignment between the text of the call flow and the call flow steps captured in the figure. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | In clause 13.4.1.1, the following step needs to be fixed to match Step 2 in the figure where the NRF authorization before issuing the access token is not optional.  2. The NRF may optionally authorize the NF service consumer. It shall then generate an access token with appropriate claims included. The NRF shall digitally sign the generated access token based on a shared secret or private key as described in RFC 7515 [45].  **Proposal**: Fix step 2 text by removing the optionality to align with the figure.  2. The NRF authorizes the NF service consumer. It shall then generate an access token with appropriate claims included. The NRF shall digitally sign the generated access token based on a shared secret or private key as described in RFC 7515 [45]. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Misalignment which could lead to misinterpretation and vulnerabkle implemntation. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 13.4.1.1 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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 Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Access token request before service access**

The following procedure describes how the NF service consumer obtains an access token before service access to NF service producers of a specific NF type.

Pre-requisite:

a. The NF Service consumer (OAuth2.0 client) is registered with the NRF (Authorization Server).

b. The NF Service Producer (OAuth2.0 resource server) is registered with the NRF (Authorization Server) with "additional scope" information per NF type.

c. The NRF and NF service producer share the required credentials.

d. The NRF and NF have mutually authenticated each other.



Figure 13.4.1.1-1: NF service consumer obtaining access token before NF service access

1. The NF service consumer shall request an access token from the NRF in the same PLMN using the Nnrf\_AccessToken\_Get request operation. The message shall include the NF Instance Id(s) of the NF service consumer, the requested "scope" including the expected NF service name(s) and optionally "additional scope" information (i.e. requested resources and requested actions (service operations) on the resources), NF type of the expected NF producer instance and NF consumer. The service consumer may also include a list of NSSAIs or list of NSI IDs for the expected NF producer instances.

The message may include the NF Set ID of the expected NF Service Producer instances.

2. The NRF authorizes the NF service consumer. It shall then generate an access token with appropriate claims included. The NRF shall digitally sign the generated access token based on a shared secret or private key as described in RFC 7515 [45].

The claims in the token shall include the NF Instance Id of NRF (issuer), NF Instance Id of the NF Service consumer (subject), NF type of the NF Service producer (audience), expected service name(s), scope (scope), expiration time (expiration) and optionally "additional scope" information (allowed resources and allowed actions (service operations) on the resources). The claims may include a list of NSSAIs or NSI IDs for the expected NF producer instances. The claims may include the NF Set ID of the expected NF service producer instances.

3. If the authorization is successful, the NRF shall send access token to the NF service consumer in the Nnrf\_AccessToken\_Get response operation,otherwise it shall reply based on Oauth 2.0 error response defined in RFC 6749 [43]. The other parameters (e.g., the expiration time , allowed scope ) sent by NRF in addition to the access token are described in TS 29.510 [68].

The NF service consumer may store the received token(s). Stored tokens may be re-used for accessing service(s) from producer NF type listed in claims (scope, audience) during their validity time.

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