**3GPP TSG-SA3 Meeting #101-e *draft\_S3-202808-r6***

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

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  |  | **CR** | **0955** | **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:*** | NRF authorization during NF service consumer Access Token Get Request | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | , Nokia, Nokia Shanghai Bell | | | | | | | | | |
| ***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, 13.4.1.2 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | | S3-202808-r6 | | | | | | | | |

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

#### 13.4.1.1 Service access authorization within the PLMN

OAuth 2.0 roles, as defined in clause 1.1 of RFC 6749 [43], are as follows:

a. The Network Repository Function (NRF) shall be the OAuth 2.0 Authorization server.

b. The NF service consumer shall be the OAuth 2.0 client.

c. The NF service producer shall be the OAuth 2.0 resource server.

**OAuth 2.0 client (NF service consumer) registration with the OAuth 2.0 authorization server (NRF)**

The NF service registration procedure, as defined in clause 4.17.1 of TS 23.502 [8], shall be used to register the OAuth 2.0 client (NF service consumer) with the OAuth 2.0 Authorization server (NRF), as described in clause 2.0 of RFC 6749 [43]. The client id, used during OAuth 2.0 registration, shall be the NF Instance Id of the NF.

**OAuth 2.0 resource server (NF service producer) registration with the OAuth 2.0 authorization server (NRF)**

The NF service registration procedure, as defined in clause 4.17.1 of TS 23.502 [8], shall be used to register the OAuth 2.0 resource server (NF Service Producer) with the OAuth 2.0 Authorization server (NRF). The NF Service Producer, as part of its NF profile, may include "additional scope" information related to the allowed service operations and resources per NF Service Consumer type.



Figure 13.4.1.1-1b NF service producer registers in NRF

1) The NF Service Producer registers as OAuth 2.0 resource server in the NRF. The NF profile configuration data of the NF Service Producer may include the "additional scope". The "additional scope" information indicates the resources and the actions (service operations) that are allowed on these resources for the NF service consumer. These resources may be per NF type of the NF Service Consumer or per NF instance ID of the NF Service Consumer.

2-3) After storing the NF Profile, NRF responds successfully.

**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 checks whether the NF service consumer is authorized to access the requested service(s). If the NF Service Consumer is authorized, the NRF 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]. If the NF Service Consumer is not authorized, the NRF shall not issue an access token to the NF Service Consumer.

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.

**Access token request for a specific NF Producer/NF Producer service instance**

The NF service consumer shall request an access token from the NRF for a specific NF Producer instance/NF Producer service instance. The request shall include the NF Instance Id(s) of the requested NF Producer, the expected NF service name, optionally "additional scope" information (allowed resources and allowed actions (service operations) on the resources) and NF Instance Id of the NF service consumer.

The NRF checks whether the NF service consumer is authorized to use the requested NF Producer instance/NF Producer service instance, and then proceeds to generate an access token with the appropriate claims included. If the NF Service Consumer is not authorized, the NRF shall not issue an access token to the NF Service Consumer.

The claims in the token shall include the NF Instance Id of NRF (issuer), NF Instance Id of the NF Service consumer (subject), NF Instance Id or several NF Instance Id(s) of the requested NF Service Producer (audience), expected service name(s) (scope) , optionally "additional scope" information (allowed resources and allowed actions (service operations) on the resources), and expiration time (expiration). The token shall be included in the Nnrf\_AccessToken\_Get response sent to the NF service consumer.

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

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of Change-2 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

#### 13.4.1.2 Service access authorization in roaming scenarios

In the roaming scenario, OAuth 2.0 roles are as follows:

a. The visiting Network Repository Function (vNRF) shall be the OAuth 2.0 Authorization server for vPLMN and authenticates the NF service consumer.

b. The home Network Repository Function (hNRF) shall be OAuth 2.0 Authorization server for hPLMN and generates the access token.

c. The NF service consumer in the visiting PLMN shall be the OAuth 2.0 client.

d. The NF service producer in the home PLMN shall be the OAuth 2.0 resource server.

**OAuth 2.0 client (NF service consumer) registration with the OAuth 2.0 authorization server (NRF) in the vPLMN**

Same as in the non-roaming scenario in 13.4.1.1.

**OAuth 2.0 resource server (NFService Producer) registration with the OAuth 2.0 authorization server (NRF) in the hPLMN**

Same as in the non-roaming scenario in 13.4.1.1.

**Obtaining access token independently before NF service access**

The following procedure describes how the NF service consumer obtains an access token for NF service producers of a specific NF type for use in the roaming scenario.



Figure 13.4.1.2-1: NF service consumer obtaining access token before NF service access (roaming)

Pre-requisite:

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

b. The hNRF and NF service producer share the required credentials. Additionally, the NF Service producer (OAuth2.0 resource server) is registered with the hNRF (Authorization Server in the hPLMN) with "additional scope" information per NF type.

c. The two NRFs have mutually authenticated each other.

d. The NRF in the serving PLMN and NF service consumer have mutually authenticated each other.

1. The NF service consumer shall invoke Nnrf\_AccessToken\_Get Request (NF Instance Id 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, NF type of the NF consumer, home and serving PLMN IDs, optionally list of NSSAIs or list of NSI IDs for the expected NF producer instances, optionally NF Set ID of the expected NF service producer) from NRF in the same PLMN.

2. The NRF in serving PLMN shall identify the NRF in home PLMN (hNRF) based on the home PLMN ID, and request an access token from hNRF as described in clause 4.17.5 of TS 23.502 [8]. The vNRF shall forward the parameters it obtained from the NF service consumer, including NF service consumer type, to the hNRF.

3. The hNRF checks whether the NF service consumer is authorized to access the requested service(s). If the NF Service Consumer is authorized, the hNRF shall generate an access token with appropriate claims included as defined in clause 13.4.1.1. The hNRF shall digitally sign the generated access token based on a shared secret or private key as described in RFC 7515 [45]. If the NF service consumer is not authorized, the hNRF shall not issue an access token to the NF Service Consumer.

The claims in the token shall include the NF Instance Id of NRF (issuer), NF Instance Id of the NF Service consumer appended with its PLMN ID (subject), NF type of the NF Service Producer appended with its PLMN ID (audience), expected services name(s),scope (scope) and 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.

4. If the authorization is successful, the access token shall be included in Nnrf\_AccessToken\_Get Response message to the vNRF. Otherwise it shall reply based on Oauth 2.0 error response defined in RFC 6749 [43]. 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. 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].

5. The vNRF shall forward the Nnrf\_AccessToken\_Get Response or error message to the NF service consumer.

**Obtain access token for a specific NF Producer/NF Producer service instance**

The NF service consumer shall request an access token from the NRF for a specific NF Producer instance/NF Producer service instance. The request shall include the NF Instance Id of the requested NF Producer, appended with its PLMN ID, the expected NF service name and NF Instance Id of the NF service consumer, appended with its PLMN ID.

The NRF in the visiting PLMN shall forward the request to the NRF in the home PLMN.

The NRF in the home PLMN checks whether the NF service consumer is authorized to use the requested NF Producer instance/NF Producer service instance and shall then proceed to generate an access token with the appropriate claims included. If the NF Service Consumer is not authorized, the NRF in the home PLMN shall not issue an access token to the NF Service Consumer.

The claims in the token shall include the NF Instance Id of NRF (issuer), NF Instance Id of the NF Service consumer appended with its PLMN ID (subject), NF Instance Id of the requested NF Service Producer appended with its PLMN ID (audience), expected service name(s) (scope) and expiration time (expiration). The token shall be included in the Nnrf\_AccessToken\_Get response sent to the NRF in the visiting PLMN. The NRF in the visiting PLMN shall forward the Nnrf\_AccessToken\_Get response message to the NF service consumer. 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-2 \*\*\*\*\*\*\*