**3GPP TSG-SA3 Meeting #100e *draft\_S3-201679-r1***

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

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  |  | **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 changeaffects:*** | UICC apps |  | ME |  | Radio Access Network |  | Core Network | **X** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** |  | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** |  | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** |  | | | | |  | ***Date:*** | | |  |
|  |  | | | |  | |  | | |  |
| ***Category:*** | A |  | | | | | ***Release:*** | | |  |
|  | *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:*** | | Text on 13.4.1.2 is unclear because a comma is missing. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Adding a missing comma to Clause 13.4.1.2. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Unclear specification | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | Clause 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:*** | |  | | | | | | | | |

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*start of change\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

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 Resource Function (vNRF) shall be the OAuth 2.0 Authorization server for vPLMN and authenticates the NF service consumer.

b. The home Network Resource 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 (NF service 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 may optionally authorize the NF service consumer and 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].

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 may optionally authorize the NF service consumer 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.

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.

**Service access request based on token verification**

In addition to the steps described in the non-roaming scenario in 13.4.1.1, the NF service producer shall verify that the PLMN-ID contained in the API request is equal to the one inside the access token.

****

**Figure 13.4.1.2-2: NF service consumer requesting service access with an access token in roaming case**

The NF service producer shall check that the home PLMN ID of audience claim in the access token matches its own PLMN identity.

The pSEPP shall check that the serving PLMN ID of subject claim in the access token matches the remote PLMN ID corresponding to the N32-f context Id in the N32 message.

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*end of change\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***