**3GPP TSG-SA3 Meeting #108-e *draft\_S5-221842-r3***

**e-meeting, 22 - 26 August 2022**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.501** | **CR** | **1436** | **rev** | **1** | **Current version:** | **17.6.0** |  |
|  | | | | | | | | |
| *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:*** | pSEPP authorization for PLM ID in access token claim | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Nokia, Nokia Shanghai Bell | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | TEI17 | | | | |  | ***Date:*** | | | 2022-08-26 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **F** |  | | | | | ***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 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-15 (Release 15) Rel-16 (Release 16) Rel-17 (Release 17) Rel-18 (Release 18)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | 33.501 clause 13.4.1.2.2. states for roaming  "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."  In 29.573 the PLMNID\_MISMATCH requirement is only mentioned for PRINS scenarios. Thus a clarification is needed in 33.501 that this check part of the OAuth procedure in roaming is only applicable to PRINS. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Update the sentence to clarify that this is only needed for PRINS. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | if not approved, there is a misalignment between SA3 and CT4 specifications. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 13.4.1.2.2 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | | S5-221842 | | | | | | | | |

\*\*\*\*\*\*\*\*\*\*\*\*\* START OF CHANGES

13.4.1.2.2 Service Request Process

The complete service request is two-step process including requesting an access token by NF Service Consumer (Step 1, i.e. 1a or 1b), and then verification of the access token by NF Service Consumer (Step 2).

**Step 1: Access token request**

Pre-requisite:

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

- 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.

- The two NRFs are implicitly authenticated via N32 mutual authentication of SEPPs.

NOTE: vSEPP to hSEPP communication is secured via N32. Only transitive trust between vNRF and hNRF can be achieved: The vNRF and vSEPP mutually authenticate, the vSEPP and hSEPP mutually authenticate, and the hSEPP and hNRF mutually authenticate. Hence, vNRF and hNRF can only implicitly authenticate each other.

- The NRF in the serving PLMN (vNRF) has authenticated the NF Service Consumer.

For SNPNs with Credentials Holder using AUSF and UDM for primary authentication, the NF Service Consumer and the vNRF are located in the SNPN while the hNRF is located in the Credentials Holder.

**1a. Access token request for accessing services of NF Service Producers of a specific NF type**

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 13.4.1.2.2-1: NF Service Consumer obtaining access token before NF Service access (roaming)**

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 Service Producer instance, NF type of the NF Service Consumer, home and serving PLMN IDs, optionally list of NSSAIs or list of NSI IDs for the expected NF Service Producer instances, optionally NF Set ID of the expected NF Service Producer) from NRF in the same PLMN.

For SNPNs with Credentials Holder using AUSF and UDM for primary authentication, the SNPN ID of the serving SNPN is included instead of the serving PLMN ID and the SNPN ID or the PLMN ID of the Credentials Holder is included instead of the home PLMN ID.

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

For SNPNs with Credentials Holder using AUSF and UDM for primary authentication, the SNPN ID of the serving SNPN is included instead of the NF Service Consumer's PLMN ID and the SNPN ID or the PLMN ID of the Credentials Holder is included instead of the NF Service Producer's PLMN ID.

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].

5. The vNRF shall forward the Nnrf\_AccessToken\_Get Response or error 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 NF Service 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].

**1b. Obtain access token for accessing services of a specific NF Service Producer instance / NF Service Producer service instance**

The following steps describes how the NF Service Consumer obtains an access token before service access to a specific NF Service Producer instance / NF Service Producer service instance.

1. The NF Service Consumer shall request an access token from the NRF for a specific NF Service Producer instance / NF Service Producer service instance. The request shall include the NF Instance Id of the requested NF Service 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.

For SNPNs with Credentials Holder using AUSF and UDM for primary authentication, the SNPN ID of the serving SNPN is included instead of the NF Service Consumer's PLMN ID and the SNPN ID or the PLMN ID of the Credentials Holder is included instead of the NF Service Producer's PLMN ID.

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

3. The NRF in the home PLMN checks whether the NF Service Consumer is authorized to use the requested NF Service Producer instance/NF Service 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).

For SNPNs with Credentials Holder using AUSF and UDM for primary authentication, the SNPN ID of the serving SNPN is included instead of the NF Service Consumer's PLMN ID and the SNPN ID or the PLMN ID of the Credentials Holder is included instead of the NF Service Producer's PLMN ID.

4. The token shall be included in the Nnrf\_AccessToken\_Get response sent to the NRF in the visiting PLMN.

5. 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 NF Instance Id or several NF Instance Id(s) of the requested NF Service Producer listed in claims (scope, audience) during their validity time.

**Step 2: 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 13.4.1.2.2-2: 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.

For SNPNs with Credentials Holder using AUSF and UDM for primary authentication, the NF Service Producer verifies the SNPN ID of the serving SNPN contained in the API request instead of the PLMN-ID, and the SNPN ID or the PLMN ID of the Credentials Holder instead of the home PLMN ID.

The pSEPP shall check that the serving PLMN ID of subject claim in the access token matches the remote PLMN ID. If PRINS is used, this can be achieved by the pSEPP checking the PLMN ID of the serving network in the access token against the PLMN ID(s) in the N32-f context.

\*\*\*\*\*\*\*\*\*\*\*\*\* END OF CHANGES