**3GPP TSG-SA3 Meeting #100e *S3-201800-r1***

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

|  |
| --- |
| *CR-Form-v12.0* |
| **CHANGE REQUEST** |
|  |
|  | **33.501** | **CR** | 0905 | **rev** | 1 | **Current version:** | **16.3.0** |  |
|  |
| *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:***  | Authorization of NF service access |
|  |  |
| ***Source to WG:*** | Nokia, Nokia Shanghai Bell |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | 5G\_eSBA |  | ***Date:*** | 7.8.2020 |
|  |  |  |  |  |
| ***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:*** | 13.4.1.1 clarification that this applies to direct communication Structering by adding subclauses needed13.4.1.1.2 missing explanation that the request is a two step process; propose to number the steps accordingly13.4.1.1 step 2 only applies in case of success13.4.1.2 clarification that this applies to direct communication 13.4.1.3 clarification needed that applicable within PLMN13.4.1.3.1.1 step 0 and 5 clarification and correction neededIn general alignment of consistantly using NFc/NFp and CCA-revision to undo the change on NFc/NFp |
|  |  |
| ***Summary of change:*** | Editorial updates in line with reason of changeClarification updates in 13.4.1.3.1.1 Discovery of NF service produce: Step 0: I.e. if the NFc has not yet discovered the NFp/NFp instance, then it may run the discovery procedure.step 5: The SCP selects a NFp instance (i.e. if the NF Service Consumer had initially selected only the NF Service Producer set),… |
|  |  |
| ***Consequences if not approved:*** | Misunderstanding of spec |
|  |  |
| ***Clauses affected:*** | 13.4.1.0, 13.4.1.1, 13.4.1.1.1 (new), 13.4.1.1.2 (new), 13.4.1.2, 13.4.1.2.1 (new), 13.4.2.2 (new), 13.4.1.4, 13.4.1.3.1.1, 13.4.1.3.1.2, 13.4.1.3.2  |
|  |  |
|  | **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:*** | Revision of S3-201800 |

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

13.4 Authorization of NF service access

13.4.1 OAuth 2.0 based authorization of Network Function service access

13.4.1.0 General

The authorization framework introduced in the following allows NF service producers to authorize the requests from NF Service Consumer. It

The authorization framework uses the OAuth 2.0 framework as specified in RFC 6749 [43]. Grants shall be of the type Client Credentials Grant, as described in clause 4.4 of RFC 6749 [43]. Access tokens shall be JSON Web Tokens as described in RFC 7519 [44] and are secured with digital signatures or Message Authentication Codes (MAC) based on JSON Web Signature (JWS) as described in RFC 7515 [45].

The basic extent provided by the authorization token is at service level (i.e. the "scope" claim includes allowed services per NF type). Depending on the NF Service Producer configuration, higher level of granularity for the authorization token can be defined adding "additional scope" information within the token e.g. to authorize specific service operations and/or resources/data sets within service operations per NF Service Consumer type.

NOTE 1: The additional scope(s) included within the access token add additional security checks at the NF Service Producer that authorizes the services operations, resources and NF Service Consumer type related to the additional scope(s).

13.4.1.1 Service access authorization within the PLMN in direct communication scenario

##### 13.4.1.1.1 OAuth 2.0 roles

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

a. The Network Resource 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.

##### 13.4.1.1.2 Service Request Process

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

**Step 1**

**1a. Access token request before service access**

The following procedure describes how the NF Service Consumer obtains an access token before granting 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 Service Consumer have mutually authenticated each other.

e. The NRF has responded to the Discovery Request sent by the NF Service Consumer.

****

**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 Service Producer instance and the NF type of the NF Service Consumer. The NF Service Consumer may also include a list of NSSAIs or list of NSI IDs for the expected NF Service Producer instances.

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

2. The NRF may optionally authorize the NF Service Consumer. If successful, 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 Service Producer instances. The claims may include the NF Set ID of the expected NF Service Producer instances.

3. If the authorization was 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.

**1b. Access token request for a specific NF Service Producer/NF Service Producer service instance**

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(s) of the requested NF Service 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 may optionally authorize the NF Service Consumer to use the requested NF Service Producer instance/NF Producer service instance, and then proceeds 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 (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.

**Step 2. Service access request based on token verification**

The following figure and procedure describe how authorization is performed during service request of the NF Service Consumer.

****

**Figure 13.4.1.1-2: NF service consumer requesting service access with an access token**

Pre-requisite: The NF Service Consumer is in possession of a valid access token before requesting service access from the NF Service Producer.

1. The NF Service Consumer requests service from the NF Service Producer. The NF Service Consumer shall include the access token.

The NF Service Consumer and NF Service Producer shall mutually authenticate following clause 13.3.

2. The NF Service Producer shall verify the token as follows:

 - The NF Service Producer ensures the integrity of the token by verifying the signature using NRF's public key or checking the MAC value using the shared secret. If integrity check is successful, the NF Service Producer shall verify the claims in the token as follows:

NOTE: Void.

- It checks that the audience claim in the access token matches its own identity or the type of NF service producer. If a list of NSSAIs or list of NSI IDs is present, the NF Service Producer shall check that it serves the corresponding slice(s).

- If an NF Set ID present, the NF Service Producer shall check the NF Set ID in the claim matches its own NF Set ID.

- If scope is present, it checks that the scope matches the requested service operation.

- If the access token contains "additional scope" information (i.e. allowed resources and allowed actions (service operations) on the resources), it checks that the additional scope matches the requested service operation.

- It checks that the access token has not expired by verifying the expiration time in the access token against the current data/time.

3. If the verification is successful, the NF Service Producer shall execute the requested service and responds back to the NF Service Consumer. 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 NF Service Producer type listed in claims (scope, audience) during their validity time.

13.4.1.2 Service access authorization in roaming scenarios in direct communication

##### 13.4.1.2.1 OAuth 2.0 roles

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.

##### 13.4.1.2.2 Service Request Process

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

**Step 1**

**1a. Obtaining access token independently before NF service access**

The following procedure describes how the NF Service Consumer obtains an access token for NF Service Producer 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 vPLMN (visited 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 Service 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 vPLMN 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 generated by the hNRF 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.

**1b. Obtain access token for a specific NF Service Producer/NF Service 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 Service Producer instance/NF Service 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.

**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 of the vPLMN contained in the NF service 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.

13.4.1.3 Service access authorization in indirect communication scenarios

13.4.1.3.1 Authorization for indirect communication without delegated discovery procedure

13.4.1.3.1.1 With mutual authentication between NF Service Consumer and NRF at the transport layer

This clause covers the scenario where the NF Service Consumer and the NRF are connected over a mutually authenticated TLS connection.

****

**Figure 13.4.1.3.1.1-1: Authorization and service invocation procedure, for indirect communication without delegated discovery, with mutual authentication between NF and NRF at the transport layer**

**Discovery of the NF Service Producer:**

0. Optionally, the NF Service Consumer may discover the NF Service Producer before requesting authorization to invoke the services of the NF Service Producer. I.e. if the NFc has not yet discovered the NFp/NFp instance, then it may run the discovery procedure.

**NF Service Consumer authorization:**

 1-2.

After mutual authentication between NF Service Consumer and NRF at the transport layer, the NF Service Consumer and NRF perform the "Access token request before service access" procedure as described in clause 13.4.1.1. If the NF Service Consumer has already discovered the NF Service Producer, it can also perform the "Access token request for a specific NF Service Producer/NF Service Producer instance" procedure as described in clause 13.4.1.1.

**Service request:**

The NF Service Consumer, SCP, NRF and NF Service Producer perform the procedure "Indirect Communication without delegated discovery Procedure" described in clause 4.17.11 of TS 23.502 [8]. The following steps describe how the access token received from steps 1 and 2 is used in this procedure.

3. If no cached data is available, the NF Service Consumer discovers the NF Service Producer (optional via the SCP).

4. The NF Service Consumer sends a service request for the specific service to the SCP. The service request includes the access token as received in step 2, and may include the NF Service Consumer CCA as defined in clause 13.3.8.

5. The SCP selects a NF Service Producer instance (i.e. if the NF Service Consumer had initially selected only the NF Service Producer set), performs the API root modifications and forwards the received request to the selected NF Service Producer instance. The request contains the access token and may contain the NF Service Consumer CCA if received in step 4.

6. To authorize the access, the NF Service Producer authenticates the service consumer NF using one of the methods described in clause 13.3.2.2 and if successful, it validates the access token as described in clause 13.4.1.1 by verifying the signature and checking if the requested service is part of the token's scope.

7. If the checks in step 6 are successful, the NF Service Producer processes the service request and provides a service response.

8. The SCP performs reverse API root modifications and forwards the service response.

13.4.1.3.1.2 Without mutual authentication between NF and NRF at the transport layer

When there is no mutual authentication between NF Service Consumer and NRF at the transport layer, the NF Service Consumer performs the following procedure to obtain the access token from NRF and uses it for service access at the NF Service Producer. In this clause, the authentication of NF Service Consumer by the NRF and by the NF Service Producer is based on any of the methods described in clauses 13.3.1.2 and 13.3.2.2.

****

**Figure 13.4.1.3.1.2-1: Authorization and service invocation procedure, for indirect communication without delegated discovery, without mutual authentication between NF and NRF at the transport layer**

0. Optionally, the NF Service Consumer may discover the NF Service Producer before requesting authorization to invoke the services of the NF Service Producer.

1. The NF Service Consumer sends an access token request (Nnrf\_AccessToken\_Get Request) to the SCP with parameters as specified in 13.4.1.1. The access token request may additionally include the NF Service Consumer CCA as defined in clause 13.3.8.

2. The SCP forwards the access token request (Nnrf\_AccessToken\_Get Request) to the NRF. The request may include the NF Service Consumer CCA if received in step 1.

3. The NRF authenticates the service consumer NF using one of the methods described in clause 13.3.1.2. If the NF Service Consumer authentication is successful and the NF Service Consumer is authorized based on the NRF policy, the NRF issues an access token as described in clause 13.4.1.1. The NRF uses the NF Service Consumer NF Instance ID as the subject of the access token.

4. The NRF sends the access token to the SCP in an access token response (Nnrf\_AccessToken\_Get Response).

5. The SCP forwards the access token response (Nnrf\_AccessToken\_Get Response) to the NF Service Consumer, including the access token.

6. The NF Service Consumer sends the service request to the SCP. The service request includes the access token received in Step 5 and may include the NF Service Consumer CCA,

7. The SCP forwards the service request to the NF Service Producer. The service request includes the access token received in step 6, and may include the NF Service Consumer CCA if received in step 6.

8. The NF Service Producer authenticates the NF Service Consumer by one of the methods described in clause 13.3.2.2 and if successful, it validates the access token as described in clause 13.4.1.1.

9. If the validation of the access token is successful, the NF Service Producer sends the service response to the SCP.

10. The SCP forwards the service response to the NF Service Consumer.

13.4.1.3.2 Authorization for indirect communication with delegated discovery procedure

This clause covers the scenario where the NF Service Consumer use the SCP to discover and select the NF Service Producer instance that can process the service request.

****

**Figure 13.4.1.3.2-1: Authorization and service invocation procedure, for indirect communication with delegated discovery**

1. The NF Service Consumer sends a service request to the SCP. The service request may include the NF Service Consumer CCA as defined in clause 13.3.8.

2. The SCP may perform a service discovery with the NRF.

3. The SCP sends an access token request (Nnrf\_AccessToken\_Get Request) to the NRF. The access token request includes parameters as defined in clause 13.4.1.1. The access token request may include the NF Service Consumer CCA if received in Step 1.

4. The NRF authenticates the NF Service Consumer using one of the methods described in clause 13.3.1.2. If cNF authentication is successful and the NF Service Consumer is authorized based on the NRF policy, the NRF issues an access token as described in clause 13.4.1.1. The NRF uses the NF Service Consumer instance ID as the subject of the access token.

5. The NRF sends the access token to the SCP in an access token response (Nnrf\_AccessToken\_Get Response).

6. The SCP sends the service request to the NF Service Producer. The service request includes the access token received in Step 5, and may include the NF Service Consumer CCA if received in Step 1.

7. The NF Service Producer authenticates the NF Service Consumer by one of the methods described in clause 13.3.2.2 and if successful, it validates the access token as described in clause 13.4.1.1.

8. If the validation of the access token is successful, the NF Service Producer sends the service response to the SCP.

9. The SCP forwards the service response to the NF Service Consumer.

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