**3GPP TSG-SA3 Meeting #98e *S3-200282***

**e-meeting, 2 – 6 March 2020**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  |  | **CR** | **0755** | **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:*** | Resource Level Authorization using Access Tokens | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Ericsson, Nokia, Nokia Shanghai Bell | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | 5G\_eSBA | | | | |  | ***Date:*** | | |  |
|  |  | | | |  | |  | | |  |
| ***Category:*** |  |  | | | | | ***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:*** | | **Changes already included in the draft-CR S3-194659 are by user "Author". Changes on top of S3-194659 are by user "Ericsson".**  In Rel-15, the 5G SBA OAuth 2.0 based service access authorization framework only allows granularity of access control at service level. The "scope" claim in the access token conveys the authorized services for the requesting NF service consumer (client id).  The 5G SBA OAuth 2.0 based service access authorization framework needs to be extended to enable granularity at resource level and service operation level. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | The 5G SBA OAuth 2.0 based service access authorization framework is extended to enable granularity at resource level and service operation level as described in solution #32 in TR 33.855.  It is proposed that the the authorization token conveys not only information about authorized services but also additional information (called “additional scopes”) about authorized service operations and/or resources/data sets within service operations.  It is proposed that Stage 3 defines how the “additional scope” information is included within the authorization token. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | The 5G SBA OAuth 2.0 based service access authorization framework does not enable granularity at resource level and service operation level. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 13.4.1.0, 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:*** | |  | | | | | | | | |

**\*\*\*\* 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 described in clause 13.4.1 allows NF service producers to authorize the requests from NF service requestors.

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 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 consumer type related to the additional scope(s).

The authorization framework described in clause 13.4.1 is mandatory to support for NRF and NF.

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 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 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 (HTTP methods) that are allowed on these resources for the NF service consumer. These resources may be per NF type of the consumer or per NF instance ID of the consumer.
   1. 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) with its NF type.

1. 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 (HTTP methods) 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 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].

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 (HTTP methods) 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 (HTTP methods) 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 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 (HTTP methods) on the resources, and expiration time (expiration). The token shall be included in the Nnrf\_AccessToken\_Get response sent to the NF service consumer.

**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. Prior to the request, the NF service consumer may perform Nnrf\_NFDiscovery\_Request operation with the requested additional scopes to select a suitable NF service producer (resource server) which is able to authorize the Service Access request.

****

**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 authenticate each other 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 (HTTP methods) 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 producer NF type listed in claims (scope, audience) during their validity time.

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 (HTTP methods) 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 (HTTP methods) 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 CHANGES \*\*\*\***