**3GPP TSG-SA3 Meeting #102-e *S3-211888-r1***

**e-meeting, 18 - 29 January 2021, Online**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.501** | **CR** | **1124** | **rev** | **1** | **Current version:** | **15.12.0** |  |
|  | | | | | | | | |
| *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:*** | Oauth client registration | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | S3 | | | | | | | | | |
| ***Source to TSG:*** | Huawei, HiSilicon, Mavenir | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | 5GS\_Ph1-SEC | | | | |  | ***Date:*** | | | 2021-04-01 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | F |  | | | | | ***Release:*** | | | Rel-15 |
|  | *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:*** | | Currently, it is still not clear on how to implement the token authorization for NRF serivces, and the Oauth client registration may not be able to be performed if the NF does not need to register with the NRF. Furthermore, how to authorize the NF during the token request procedure needs to be further illustrated. Hence, it is proposed to clarify the above unclear statements. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Changing the Note to a normative language, that token for NRF serivce are not required.  Clarify how to implement the Oauth client registration. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Unclear specification. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 13.3.1, 13.4.1.1.2, 13.4.1.2.2 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **Y** | **N** |  | | | |  | | |
| ***Other specs*** | |  |  | Other core specifications | | | | TS/TR ... CR ... | | |
| ***affected:*** | |  |  | Test specifications | | | | TS/TR ... CR ... | | |
| ***(show related CRs)*** | |  |  | O&M Specifications | | | | TS/TR ... CR ... | | |
|  | |  | | | | | | | | |
| ***Other comments:*** | |  | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | |  | | | | | | | | |

\*\*\*\*\*\*\*\*\*\*\*\*\*\*Start of the first change\*\*\*\*\*\*\*\*\*\*\*\*\*\*

### 13.3.1 Authentication and authorization between network functions and the NRF

NRF and NF shall authenticate each other during discovery, registration, and access token request. If the PLMN uses protection at the transport layer as described in clause 13.1, authentication provided by the transport layer protection solution shall be used for mutual authentication of the NRF and NF.

If the PLMN does not use protection at the transport layer, mutual authentication of NRF and NF may be implicit by NDS/IP or physical security (see clause 13.1).

When NRF receives message from unauthenticated NF, NRF shall support error handling, and may send back an error message. The same procedure shall be applied vice versa.

After successful authentication between NRF and NF, the NRF shall decide whether the NF is authorized to perform discovery and registration.

In the non-roaming scenario, the NRF authorizes the Nnrf\_NFDiscovery\_Request based on the profile of the expected NF/NF service and the type of the NF Service Consumer, as described in clause 4.17.4 of TS 23.502 [8].In the roaming scenario, the NRF of the NF Service Producer shall authorize the Nnrf\_NFDiscovery\_Request based on the profile of the expected NF/NF Service, the type of the NF Service Consumer and the serving network ID.

If the NRF finds NF Service Consumer is not allowed to discover the expected NF instances(s) as described in clause 4.17.4 of TS 23.502[8], NRF shall support error handling, and may send back an error message.

When a NF accesses any services (e.g. register, discover or request access token) provided by the NRF, the NRF shall use the static authorization policy to authorize the service request sent by the NF. Therefore, the OAuth 2.0 access token for authorization between the NF and the NRF is not needed and the NF shall not request an access token for consuming the NRF services. The NF may however request an access token from the NRF for consuming other NF producer services.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*End of the first change\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*Start of the second change\*\*\*\*\*\*\*\*\*\*\*\*\*\*

## 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 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].

NOTE 1: Securing the access token using Message Authentication Codes (MAC) based on JSON Web Signature (JWS) as described in RFC 7515 [45] requires a pairwise pre-shared symmetric key between the NRF and the NF Service Producer. The provisioning of such pre-shared symmetric key is outside the scope of this document.

The authorization framework described in clause 13.4.1 shall be supported for NRF and NF.

#### 13.4.1.1 Service access authorization within the PLMN

##### 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 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] in the following cases: (a) the NF Service Consumer is subscribing to notification services at the NRF and (b) if the NF Service Consumer is also acting as a NF Service Producer. Otherwise, the OAuth 2.0 client (NF Service Consumer) registration procedure is not required Static authorization can be used for the OAuth 2.0 client (NF Service Consumer) authorization by the NRF. The client id, used during OAuth 2.0 registration, shall be the NF Instance Id of the NF.

##### 13.4.1.1.2 Service Request Process

The complete service request is a 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 Producer (Step 2).

**Step 1:**

Pre-requisite:

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

- The NRF and NF service producer share the required credentials.

- The NRF and NF have mutually authenticated each other.

**1a. 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.



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, expected NF Service name(s), NF type of the expected NF Service Producer instance and NF consumer. The Service Consumer may also include a list of NSSAIs or list of NSI IDs for the expected NF Service Producer instances.

2. The NRF authorizes the NF service consumer by verifying the input parameters (e.g., NF type) in the access token request match with the corresponding ones in the public key certificate of the NF service consumer or that in the NF profile of the NF service consumer, and authorizes the NF service consumer as the OAuth client based on the static authorization policy, or based on the OAuth 2.0 client registration profile received during the NF Service registration procedure, as specified in clause 13.4.1.1.1. 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) and expiration time (expiration). The claims may include a list of NSSAIs or NSI IDs for 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 NF Service Producer NF type listed in claims (scope, audience) during their validity time.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*End of the second change\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*Start of the third change\*\*\*\*\*\*\*\*\*\*\*\*\*\*

#### 13.4.1.2 Service access authorization in roaming scenarios

##### 13.4.1.2.1 OAuth 2.0 roles

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.

##### 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**

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 have mutually authenticated each other.

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

**1a. 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)

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.

2. The NRF in serving PLMN authorizes the NF service consumer by verifying the input parameters (e.g., NF type) in the access token request match with the corresponding ones in the public key certificate of the NF service consumer or that in the NF profile of the NF service consumer, and authorizes the NF service consumer as the OAuth client based on the static authorization policy, or based on the OAuth 2.0 client registration profile received during the NF Service registration procedure, as specified in clause 13.4.1.2.2, 1a. If the authorization is successful, 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) based on the static authorization policy. 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 Service 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 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].

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

\*\*\*\*\*\*\*\*\*\*\*\*\*\*End of the third change\*\*\*\*\*\*\*\*\*\*\*\*\*\*