**3GPP TSG-SA3 Meeting #116 *S3-242461-r2***

Jeju, South Korea, 20 - 24 May 2024

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  |  | **CR** |  | **rev** | **2** | **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:***  | Clarifications on NRF and NFp checks |
|  |  |
| ***Source to WG:*** | Nokia, Nokia Shanghai Bell |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | 5G\_eSBA\_Ph2 |  | ***Date:*** | 2024-05-24 |
|  |  |  |  |  |
| ***Category:*** | **F** |  | ***Release:*** | Rel-18 |
|  | *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-15 (Release 15)Rel-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)* |
|  |  |
| ***Reason for change:*** | SBA study 33.875 KI#11 discussed topic on matching certificate details with requests (NRF management, access token and service request) was concluded with focus on NF Instance Id, NF Type and PLMN id if available. This needs further explanation in specification text.Note, the specification should provide precise reference to existing spec IEs or certificate details that are matched. |
|  |  |
| ***Summary of change:*** | To the requirements on NRF (5.9.2.2) a clarification NOTE 1 is added and precise validation rules for NRF wrt certificates and CCA are provided. With this, 13.4.1.1.2 can be simplified to reference 5.9.2 wrt the matching of input parameters with the corresponding ones in the public key certificate of the NF Service Consumer.Managing NF profile and checking against certificate information has been addressed by NOTE 1, hence in 13.4.1.1.2 this part on NF profile verification is removed, since it should be the pre-assumption already. |
|  |  |
| ***Consequences if not approved:*** | Revisiting the same key isssue in Rel-19 again.  |
|  |  |
| ***Clauses affected:*** | 13.4.1.1.1, 13.4.1.1.2 |
|  |  |
|  | **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:*** | Implement after updates in 2452, 2462 |
|  |  |
| ***This CR's revision history:*** | ***S3-241842*** |

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

##### 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], may 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].

NOTE 1: If the NF Profile of the NF Service Consumer is registed at the same NRF, the NRF can verify whether the values of parameters are present both in the NF profile and in the public key certificate of the NF instance. This is implementation specific.

The client id, used during OAuth 2.0 registration, shall be the NF Instance Id of the NF. OAuth2.0 clients may also register with the NRF using OAM.

A Network Function that does not implement this option shall be able to get an access token from the NRF as long as the NRF is able to authenticate and authorize the Network Function during the NF access token get service request.

**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.

\*\*\*\*\*\*\*\*\*\*\*\*\*\* NEXT CHANGE

##### 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).

NOTE: The service request process regarding the enabler for network automation is specified in Annex X.

**Step 1: Access token request**

Pre-requisite:

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

- The NF Service Producer (OAuth2.0 resource server) is registered with the NRF (Authorization Server) with optionally "additional scope" information per NF type.

- The NRF and NF Service Producer share the required credentials.

- The NRF and NF have mutually authenticated each other – where the NF Service Consumer is identified by the NF Instance ID of the public key certificate of the NF Service Consumer.

**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 before service access to NF Service Producers of a specific NF type.



Figure 13.4.1.1.2-1: 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 NF Service Consumer. The NF Service Consumer may also include a list of S-NSSAIs or list of NSI IDs for the expected NF Service Producer instances.

The message may include the NF Set ID and/or NF Service Set Id of the expected NF Service Producer instances.

The message may include a list of S-NSSAIs of the NF Service Consumer.The message may also include the

PLMN ID(s) of the NF Service Consumer.

2. The NRF shall verify that the input parameters NF Instance ID and NF type as well as PLMN ID(s), if available, in the access token request match with the corresponding ones in the public key certificate of the NF Service Consumer, or those in the NF profile of the NF Service Consumer if the NF Service Consumer profile is registered at the same NRF. If the verification of the parameters in the access token request fails, the access token request is not further processed.

The NRF shall may additionally verify the S-NSSAIs of the NF Service Cons and check whether there are restrictions on the NF Service Consumer to access NF Service Producers' services of a specific NF type depending on the slices for which they offer their services umer. The NRF checks whether the NF Service Consumer is authorized to access the requested service(s). For example, the NRF may verify that the NF Service Consumer can serve a slice which is included in the allowed slices for the NF Service Producer of a specific NF type. 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), 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 S-NSSAIs or NSI IDs for the expected NF Service Producer instances. The claims may include the NF Set ID and/or NF Service Set Id of the expected NF Service Producer instances.

NOTE: If the claims do not include a list of NSSAIs or NSI IDs for the target NF type, it implies the token can be used to access expected NF services of all expected NF Service Producers of the NF type based on local configuration and operator policy.

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.

**1b. Access token request 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(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 request may also include the PLMN ID(s) of the NF Service Consumer.

2. The NRF shall verify that the input parameters in the access token request, i.e. NF Instance ID and, if available, PLMN ID(s) and NF type, match with the corresponding ones in the public key certificate of the NF Service Consumer or those in the NF profile of the NF Service Consumer, if the NF Service Consumer profile is registered at the same NRF. If the verification of the parameters in the access token request fails, the access token request is not further processed.

The NRF checks whether the NF Service Consumer is authorized to access the requested services from the NF Service Producer instance/NF Service Producer service instance, and then proceeds to generate an access token with the appropriate claims included. 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 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).

3. The token shall be included in the Nnrf\_AccessToken\_Get response sent 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 instance listed in claims (scope, audience) during their validity time.

**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. 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 13.4.1.1.2-2: 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: -

 In the direct communication case, it checks that the NF Instance ID in the subject claim within the access token matches the NF Instance ID in the subjectAltName in the NF Service Consumer's TLS client certificate.

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 ofS-NSSAIs or list of NSI IDs is present, the NF Service Producer shall check that it serves the corresponding slice(s). If applicable (e.g., when the request is for information related to a specific UE), the NF Service Producer may check that the NF Service Consumer is allowed to access (as indicated by the NF Service Producer’s S-NSSAIs in the access token presented by the NF Service Consumer) at least one of the slice(s) that the UE is currently registered to, e.g., by verifying that the UE’s allowed NSSAI(s) intersect with the NF Service Producer's S-NSSAIs in the access token.

- 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 an NF Service Set ID present, the NF Service Producer shall check if the NF Service Consumer is authorized to access the requested service according to NF Service Producer Service Set ID in the access token claim.

- 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.

- If the CCA is present in the service request, it may verify the CCA as specified in clause 13.3.8.3 and that the subject claim (i.e., the NF Instance Id of the NF Service Consumer) in the access token matches the subject claim in the CCA.

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].

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