**3GPP TSG-SA3 Meeting #115 *S3-240867-r2***

**Athens, Greece, 26 February - 01 March 2024**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  |  | **CR** | **1946** | **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:*** | Consistency Between NF Profile and Certificate | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Ericsson, Deutsche Telekom, China Telecom, KDDI, Nokia, Nokia Shanghai Bell, CableLabs | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | 5G\_eSBA\_Ph2 | | | | |  | ***Date:*** | | | 2024-02-19 |
|  |  | | | |  | |  | | |  |
| ***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 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:*** | | An NF can use the service operation Nnrf\_NFManagement\_NFRegister\_request (for brevity, referred to as register request) provided by the NRF to register the NF’s profile when the NF becomes operative for the first time. The NF can also use the service operation Nnrf\_NFManagement\_NFUpdate\_request (for brevity, referred to as update request) of the NRF to update the NF’s already-registered NF profile. This update may be triggered, for example, after a scaling operation. Clauses 4.17.1 and 4.17.2 in TS 23.502 describe these two service operations in detail, and Clauses 5.2.7.2.2 and 5.2.7.2.3 in TS 23.502 describe input parameters that the NF can send in the register and update request. The parameters which must be (and can be) present in the NF’s certificate profile are presented in TS 33.310, Table 6.1.3c.3-1: NF TLS Client and Server Certificate Profile.  The NOTE 3 in Clause 4.17.1 in TS 23.502 states that whether the NF profile sent by NF to NRF needs to be integrity protected by the NF and verified by the NRF is to be decided by SA3. The values of the NF profile parameters that are sent by the NF in the register and update requests should be consistent with the values of those parameters, if present, in the TLS client certificate associated with the NF that the NRF uses to authenticate the NF.  The consistency between the profile and certificate is important because, otherwise, an NF Service Consumer can change important parameters in its NF profile at the NRF, whenever it wishes, to obtain an access token to access a service that the NF Service Consumer is not entitled to. The current specification does not include any requirements (or verification steps) towards ensuring that the profile and certificate of an NF are consistent with each other.  In the current specification of token-based authorization, the NRF only cross-checks certain input parameters of the access token request with the certificate or profile of the NF Service Consumer sending the access token request. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | A note for clarifying NRF security requirements to ensure that NF profile and Certificate never have inconsistent values for the attributes that are present both in the NF profile and certificate.  Clarifies that the NRF checks all input parameters in the access token request. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | A malicious NF instance may modify its NF profile at the NRF to obtain access token that the NF instance is not entitled to obtain. An erroneous NF instance may update its NF profile in a mistakenly (i.e., not maliciously) wrong way.  Not all input parameters of the access token request will be cross-checked with verified information about the NF Service Consumer sending the access token request. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 5.9.2.2, 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:*** | |  | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | |  | | | | | | | | |

\*\*\* BEGIN CHANGES OF 1 \*\*\*

#### 5.9.2.2 NRF security requirements

The Network Repository Function (NRF) receives NF Discovery Request from an NF instance, provides the information of the discovered NF instances to the NF instance, and maintains NF profiles. The NRF receives from NF Service Consumers or SCPs access token requests for service consumption and provides authorization tokens.

The NRF shall act as authorization server.

The following NRF service-based architecture security requirements shall apply:

NRF and NFs that are requesting service shall be mutually authenticated.

NRF may provide authentication and authorization to NFs for establishing secure communication between each other.

NOTE: An NF instance can register or update its profile in an NRF using NFRegister and NFUpdate request as specified in clauses 4.17.1 and 4.17.2 of TS 23.502 [8]. Before storing a new NF profile (in the case of NFRegister request) or updating an existing NF profile (in the case of NFUpdate request) of an NF instance, the NRF checks the consistency between the NFRegister/NFUpdate request and the TLS certificate of the NF instance for the attributes that are present in both. The consistency checks include, but are not limited to (i) when an attribute (e.g., NF type) can take only a single value, the value of such attribute in the NFRegister/Update request and the NF TLS certificate needs to same, and (ii) in the case that an attribute can take a set of values, each value of such attribute in the NFRegister/Update request needs to be present in the NF’s TLS certificate. If the NRF detects an inconsistency, it can reject the request. If an attribute in the NFRegister/NFUpdate request is not present in the NF TLS certificate, the NRF can allow for the attribute.

\*\*\* END CHANGES OF 1 \*\*\*

\*\*\* BEGIN CHANGES \*\*\*

##### 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 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 in the access token request, including, but not limited to, NF Instance ID, NF type, PLMN ID(s), and S-NSSAIs, if available, 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 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 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. 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 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.

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, including, but not limited to, NF Instance ID, PLMN ID(s) and NF type, if available, 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 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 of 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 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 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 CHANGES \*\*\*