**3GPP TSG-SA3 Meeting #119 draft\_S3-245334-r1**

Orlando, US, 11 -15 November 2024

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.501** | **CR** | **DRAFT** | **rev** | **-** | **Current version:** | **19.0.0** |  |
|  | | | | | | | | |
| *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:*** |  | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Ericsson, Deutsche Telekom, AT&T, Samsung, BT PLC, KDDI, Huawei, NCSC, Nokia | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | TEI19 | | | | |  | ***Date:*** | | | 2024-11-04 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **B** |  | | | | | ***Release:*** | | | Rel-19 |
|  | *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:*** | | As specified in the 3GPP, 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].  Currently, the information related to the public keys needed to verify the signature in the access token is assumed to be configured manually at the NFp. Manual configuration does not scale well and is error-prone. This is a concern in large real-world deployments, especially in those that have layered structured NRFs and use key rotation.  And it is also not clear how the NF producer can know that the NRF in the issuer claim of an access token is authorized to issue the access token. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | The public key used to verify the access token signature can be provided by the NRF in an X.509 certificate through a new service request and response.  Clarify that NFp need verify that the access token is issued by the OAuth 2.0 authorization server, which can be the NRF that the NFp registered at, or the NRF that is not registered at but locally configured as authorized OAuth 2.0 authorization server. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | No specification about how to distribute the public key that can verify the digital signature of the access token.  No specification about issuer claim verification of the access token. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 13.4.1.0, 13.4.1.1.1, 13.4.1.1.2, 14.3.1 and 14.3.X (new) | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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 OF CHANGES 1 \*\*\*

#### 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. Subscription requests are also service requests.

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 1a: 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.

Editor’s Note: If retrieval of keys is important, also pre-shared key retrieval has to be addressed or not is FFS. FFS how to use a symmetric key in case of NF Sets and for NF type level access.

NOTE X: Securing the access token using digital signature based on JSON Web Signature (JWS) as described in RFC 7515 [45] requires a public/private key pair at the NRF and the public key of NRF at the NF Service Producer to allow the NF Service Producer to verify the digital signature of the access token. The provisioning of the NF Service Producer with the public key of the NRF (through an X.509 certificate) to the NF Service Producer can be done for example by OAM, by using the service operation specified in clause 14.3.X or in any other implementation specific way outside the scope of this document.

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).

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

The OAuth 2.0 framework does not apply to the notification operation.

Extensions to the authorization framework specific for the security of enablers for Network Automation by 5GS are described in Annex X.

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

\*\*\* BEGIN OF CHANGES 2 \*\*\*

##### 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]. 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.

Editor’s Note: How NF determines which NRFs or NRF Sets are allowed to act as authorization servers is ffs. Details of information to be configuered in the NF Service Producer are ffs.

2-3) After storing the NF Profile, NRF responds successfully.

Editor’s Note: Whether the NF Service Producer can be registered at an OAuth 2.0 authorization server (NRF) that is different from the NRF that will issue an access token for accessing the services of this NF Service Producer is FFS. If this is the case, specification pre-requisites updates and further considerations are needed, because the current assumption is that the NF is registered at the authorization server that issues the access token. Further, since it is assumed that each NRF has its own public/private key pair, it is FFS how to configure the NF Service Producer for access token validation from a different NRF. This includes NRF Sets or an access token issued by a NRF that is not part of the NRF Set the NF Service producer is registered with.

Editor’s note: How NRF determines target NRF for forwarding tokens for NF type access in deployments with several NRFs is FFS.

\*\*\* END OF CHANGES 2 \*\*\*

\*\*\* BEGIN OF CHANGES 3 \*\*\*

##### 

##### 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 1a: 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).

The message shall include the 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 in the access token request. 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 verification of the parameters in the access token request fails, the access token request is not further processed.

The NRF shall additionally verify the S-NSSAIs of the NF Service Consumer 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. 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 1: 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.

NOTE 2: The expiration time claim (expiration) of the token is to impose time limits on the access token in use. It is carefully chosen based on the operator’s policy to allow flexibility and cost effectiveness, taking into consideration different threat situations and network complexities etc. In the present document, token revocation is not supported.

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**

1. 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 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. The NRF shall additionally verify the S-NSSAIs of the NF Service Consumer and check whether there are restrictions on the NF Service Consumer to access NF Service Producers' services depending on the NF Service Producer's allowed slices for which they offer their services. 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 instance / NF Service Producer service instance. If the NF Service Consumer is authorized,the NRF 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 shall check that the identity in the issuer claim in the access token matches the identity of the OAuth 2.0 authorization server (NRF) that is allowed to issue access tokens to this NF Service Producer. .

Editors Note: It is FFS what are the consequences of this check. E.g. If they do not match, whether the NF Service Producer provides error cause and logging information to the NRF where the NF Service Prodcuer is registered or any other NRF or OAM.

- 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 the NF Service Producer does not have the public key or verification fails, it may request for a new public key by using the service operation specified in XXX.

Editor’s note: It is FFS what are the consequences of failure, or for which reason the public key known to NF Service Producer fails. Is it because of expiry or revocation of the cert?

- 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 3: Void.

- It checks that the audience claim in the access token matches its own identity or the NF type of NF Service Producer. If a list of S-NSSAIs or list of NSI IDs i of the NF type of the NF Service Producer s present, in the access token the NF Service Producer shall check that at least one of the S-NSSAIs or NSI IDs served by the NF Service Producer is included in the list. 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 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 3 \*\*\*

\*\*\* BEGIN OF CHANGES 4 \*\*\*

### 

### 14.3.1 General

The following table illustrates the security related services for OAuth 2.0 that NRF provides. OAuth 2.0 based authorization is described in clause 13.4.1.

|  |  |  |  |
| --- | --- | --- | --- |
| Service Name | Service Operations | Operation Semantics | Example Consumer(s) |
| Nnrf\_AccessToken | Get | Request/Response | AMF, SMF, PCF, NEF, NSSF, SMSF, AUSF |
|  | RetrieveCertificate | Request/Response | AMF, SMF, PCF, NEF, NSSF, SMSF, AUSF, NRF |

The complete list of NRF services is defined in TS 23.501 [2], clause 7.2.6, and further refined in TS 23.502 [8], clause 5.2.7.

Editor’s Note: It is FFS, if AccessToken service is the correct service for adding a management operation.

Editor’s Note: It is FFS, which fields the OAuth 2.0 token should include, e.g. URIs or key ids, to allow for identification or location of the public key/cert of the access token issuer. To be considered, certificates may be managed by a different entity than the NRF.

Editor’s Note: it is FFS, whether a NF Service Producer has only one certificate/public key available, which can result in a failure and delay for fetching a new cert/pub key or if NF Service Producers should have at least two certificates of potential access token issuers. Also to support different NF services, the NRF may have several certificates (eg slice specific).

Editor’s Note: It is FFS if a NF Service Producer should be able to subscribe for updates of NRF cert/pub keys, request status of a stored cert/pub key.

\*\*\* END OF CHANGES 4 \*\*\*

\*\*\* BEGIN OF CHANGES 5 \*\*\*

### 14.3.X Nnrf\_AccessToken\_RetrieveCertificate Service Operation

**Service Operation name:** Nnrf\_AccessToken\_RetrieveCertificate.

**Description:** NF Service Consumer requests NRF to provide public key to validate the signature of the Access Token.

**Inputs, Required:** the NF Instance Id of the token issuer NRF, the key identifier (Key ID from the Header Parameter of the JOSE header of the access token), reason for request.

**Inputs, Optional:** UUID of NF Service Producer..

**Outputs, Required:** X.509 public key certificate(s) or certificate chain(s) used for signing the access token.

**Outputs, Optional:** None.

Editor’s Note: Multiple certificates of a NRF instance may be configured to a NF Service Producer, hence input parameters in new service operations are not sufficient if one wants to fetch a particular certificate. FFS if additional parameters are needed.

Editor’s Note: An attacker may pretend to be an NRF and has issued an access token signed with its private key, not known to NF Service Producer, i.e. not previously configured at NFp and not created from the root cert. How to handle such situation at NF Service Provider is FFS.

Editor’s notes: Causes for validation failure can be several: stored certificate not valid anymore (expiry), stored certificate revoked, new cert / private key for signing used by a legitimate NRF, compromised NRF issuing a token. It is FFS how to handle validation failure.

\*\*\* END OF CHANGES 5 \*\*\*