**3GPP TSG-SA3 Meeting #123 S3-252630-r2 (merger with 2538)**

Goteborg, Sweden, 25 – 29 August 2025

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  |  | **CR** |  | **rev** | **1** | **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:*** | Clarification on access token with respect to a list of S-NSSAIs | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Huawei, HiSilicon, Nokia | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | 5G\_eSBA | | | | |  | ***Date:*** | | | 2025-08-18 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **F** |  | | | | | ***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:*** | | In “case 1a” (i.e., Access Token Request for NF Producers of a specific NF type) it is stated a list of S-NSSAIs may be included in a token claim. However, in “case 1b” (i.e., Access Token Request for specific NF Producer instance) similar description is missing. This inconsistence may cause confusion that S-NSSAI information might not be needed in “case 1b”. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Adding a similar sentence and a similar NOTE for “case 1b”. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | May cause implementation errors | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 13.4.1.1.2, 13.4.1.2.2 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | | Merger of 2630 and 2538 | | | | | | | | |

\* \* \* First 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 1a: The service request process regarding the enabler for network automation is specified in Annex X.

NOTE 1b: How the requested NRF finds the target NRF when multiple NRFs are deployed in one PLMN is described in clauses 5.4.2.2.2 and 5.4.2.2.3 of TS 29.510 [68].

**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 protect the access token as described in RFC 7515 [45] with a digital signature or a MAC. 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 issued at (iat) and "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 0: If any, only slices supported by the NF Producer and authorized for the particular NF Consumer are included in the list of S-NSSAIs or list of NSI IDs for 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**

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. The NRF shall protect the access token as described in RFC 7515 [45] with a digital signature or a MAC. 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 issued at (iat) and "additional scope" information (allowed resources and allowed actions (service operations) on the resources), and expiration time (expiration).

The claims may include a list of S-NSSAIs or NSI IDs for the expected NF Service Producer instance or the expected NF Service Producer service instance.

NOTE 0: If any, only slices supported by the NF Producer and authorized for the particular NF Consumer are included in the list of S-NSSAIs or list of NSI IDs for the expected NF Service Producer instances.

NOTE 1: If the claims do not include a list of NSSAIs or NSI IDs, it implies the token can be used to access all NSSAIs or NSIs of the expected NF Service Producer instance or the expected NF Service Producer service instance based on local configuration and operator policy.

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(s) (NRF or NRF Set) that is allowed to issue access tokens to this NF Service Producer.

- 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.

NOTE 2a: The NF Service Producer needs the required root certificate to validate the NRF’s OAuth 2.0 Access Token certificate (chain).

NOTE 2b: To validate the access token, the NF Service Producer needs the public key identified by the header parameter. If the NF Service Producer does not have the public key, the NF retrieves the key using the service operation specified in clause 14.3.3 or another means of retrieval out of scope of the present document.

NOTE 2c: Certificate validation procedures are specified in clauses 6.3 and 10.4 of TS 33.310 [5]. The permitted header parameters are specified in clause 6.3.3 of TS 33.210 [3].

- 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 of the NF type of the NF Service Producer is 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 It may decide to reject the issued access token based on "issued at" (iat) claim and local policy.

- 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]. The valid error codes are maintained by IANA in the OAuth Parameters registry.

\* \* \* Next Changes \* \* \* \*

##### 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 Producer (Step 2).

**Step 1: Access token request**

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 optionally "additional scope" information per NF type.

- The two NRFs are implicitly authenticated via N32 mutual authentication of SEPPs.

NOTE: vSEPP to hSEPP communication is secured via N32. Only transitive trust between vNRF and hNRF can be achieved: The vNRF and vSEPP mutually authenticate, the vSEPP and hSEPP mutually authenticate, and the hSEPP and hNRF mutually authenticate. Hence, vNRF and hNRF can only implicitly authenticate each other.

- The NRF in the visited PLMN (vNRF) has authenticated the NF Service Consumer. – where the NF Service Consumer is identified by the NF Instance ID of the public key certificate of the NF Service Consumer.

For SNPNs with Credentials Holder using AUSF and UDM for primary authentication, the NF Service Consumer and the vNRF are located in the SNPN while the hNRF is located in the Credentials Holder.

**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 for NF Service Producers of a specific NF type for use in the roaming scenario.



Figure 13.4.1.2.2-1: 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 S-NSSAIs or list of NSI IDs for the expected NF Service Producer instances, optionally NF Set ID and/or the NF Service Set ID of the expected NF Service Producer) from NRF in the same PLMN.

For SNPNs with Credentials Holder using AUSF and UDM for primary authentication, the SNPN ID of the serving SNPN is included instead of the serving PLMN ID and the SNPN ID or the PLMN ID of the Credentials Holder is included instead of the home PLMN ID.

2. The NRF in visited PLMN shall verify the input parameters in the access token request as described under Step 1 in clause 13.4.1.1.2. If the verification of the parameters in the access token request fails, the access token request is not further processed. After successful verification of the input parameters, the vNRF 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). 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) and expiration time (expiration), and optionally issued at (iat) and "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 the NF Service Set ID of the expected NF Service Producer instances.

For SNPNs with Credentials Holder using AUSF and UDM for primary authentication, the SNPN ID of the serving SNPN is included instead of the NF Service Consumer's PLMN ID and the SNPN ID or the PLMN ID of the Credentials Holder is included instead of the NF Service Producer's PLMN ID.

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].

5. The vNRF shall forward the Nnrf\_AccessToken\_Get Response or error 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 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].

**1b. Obtain access token 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 of the requested NF Service 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.

For SNPNs with Credentials Holder using AUSF and UDM for primary authentication, the SNPN ID of the serving SNPN is included instead of the NF Service Consumer's PLMN ID and the SNPN ID or the PLMN ID of the Credentials Holder is included instead of the NF Service Producer's PLMN ID.

2. The NRF in serving PLMN shall verify the input parameters in the access token request as described under Step 1 in clause 13.4.1.1.2. If the verification of the parameters in the access token request fails, the access token request is not further processed. After successful verification of the input parameters, the NRF in the visited PLMN shall forward the request to the NRF in the home PLMN.

3. The NRF in the home PLMN 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 shall then proceed to generate an access token with the appropriate claims included. If the NF Service Consumer is not authorized, the NRF in the home PLMN 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 Instance Id of the requested NF Service Producer appended with its PLMN ID (audience), expected service name(s) (scope) and expiration time (expiration) and optionally issued at (iat). The claims may include a list of S-NSSAIs or NSI IDs for the expected NF Service Producer instance or the expected NF Service Producer service instance.

For SNPNs with Credentials Holder using AUSF and UDM for primary authentication, the SNPN ID of the serving SNPN is included instead of the NF Service Consumer's PLMN ID and the SNPN ID or the PLMN ID of the Credentials Holder is included instead of the NF Service Producer's PLMN ID.

4. The token shall be included in the Nnrf\_AccessToken\_Get response sent to the NRF in the visited PLMN.

5. The NRF in the visited 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 NF Instance Id or several NF Instance Id(s) of the requested NF Service Producer listed in claims (scope, audience) during their validity time.

**Step 2: 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 (or SNPN ID) contained in the API request is equal to the one inside the access token.



Figure 13.4.1.2.2-2: 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.

For SNPNs with Credentials Holder using AUSF and UDM for primary authentication, the NF Service Producer verifies the SNPN ID of the serving SNPN contained in the API request instead of the PLMN-ID, and the SNPN ID or the PLMN ID of the Credentials Holder instead of the home PLMN ID.

The pSEPP shall check that the serving PLMN ID of subject claim in the access token matches the remote PLMN ID. If PRINS is used, this can be achieved by the pSEPP checking the PLMN ID of the serving network in the access token against the PLMN ID(s) in the N32-f context.

If the peer network is an SNPN, the pSEPP shall check that the SNPN ID of the NF Service Consumer in the access token matches the SNPN ID of the peer network.

\* \* \* End of Changes \* \* \* \*