**3GPP TSG-SA3 Meeting #103-e *draft\_S3-211986-r1***

**e-meeting, 17 - 28 May 2021**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.501** | **CR** | **1132** | **rev** | **1** | **Current version:** | **17.1.0** |  |
|  | | | | | | | | |
| *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:*** | Prevention of attacks on slice core by CCA modifications | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | S3 | | | | | | | | | |
| ***Source to TSG:*** | Nokia, Nokia Shanghai Bell | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | 5G\_eSBA | | | | |  | ***Date:*** | | | 2021-05-28 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **A** |  | | | | | ***Release:*** | | | Rel-17 |
|  | *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 the NSSAI ID to which a NF Service Consumer (if provided in the access token get request) belongs cannot be verified by the NRF, because the NSSAI ID is neither a part of the certificate profile of NF Service Consumer, nor can it be assured that the NRF receiving the access token request contains the profile of the NF Service Consumer from which the request is received.  Thus, network slice access violation may become possible.  Therefore, CCA as described in the clause 13.3.8 needs to have the NSSAI ID value of the NF Service Consumer included to allow the NRF to verify the NSSAI ID at least for NFs that use the CCA concept.  In addition, the access token claims generated by the NRF need to be enhanced to also include the NSSAI ID of the NF Service Consumer, so that when receiving the service request, the NF Service Producer can also verify the NSSAI ID of the NF Service Consumer by comparing the NSSAI value present in the CCA against the NSSAI value present in the access token claims. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Include Network Slice ID, i.e.S-NSSAI or NSI ID in the CCA of the service consumer. Enable NRF to verify the S-NSSAI of the service consumer in the CCA. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Network Slice access violations may become possible. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 13.3.8.2, 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:*** | |  | | | | | | | | |

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

13.3.8.2 Client credentials assertion

CCAs shall be JSON Web Tokens as described in RFC 7519 [44] and are secured with digital signatures based on JSON Web Signature (JWS) as described in RFC 7515 [45].

The CCA shall include:

- the NF instance ID of the NF Service Consumer (subject);

- A timestamp (iat) and an expiration time (exp), and

- The NF type of the expected audience (audience), i.e. the type "NRF", "NF Service Producer", or "NRF" and "NF Service Producer".

- List of NSSAIs or NSI IDs to which a NF Service Consumer belongs.

The NF Service Consumer shall digitally sign the generated CCA based on its private key as described in RFC 7515 [45]. The signed CCA shall include one of the following fields:

- the X.509 URL (x5u) to refer to a resource for the X.509 public key certificate or certificate chain used for signing the client authentication assertion, or

- the X.509 Certificate Chain (x5c) include the X.509 public key certificate or certificate chain used for signing the client authentication assertion.

\*\*\*\*\*\*\*\*\*\*\*\*\*\* 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).

**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 "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.

**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 of the expected NF Service Producer instances.

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

2. The NRF may verify that 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 NF data registered during the Oauth2 client registration. 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), 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, a list of NSSAIs or NSI IDs for the NF Service Consumer. The claims may include the NF 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.

2.The NRF checks whether the NF Service Consumer is authorized to use the requested 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:

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 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 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. It may also verify the NSSAIs or NSI IDs value present in the CCA matches the NSSAIs or NSI IDs of the NF Service Consumer present in the access token claims.

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]. If the NF Service Consumer's NSSAIs were included in access token claims, the NF Service Producer may additionally validate if the NF Service Consumer is allowed to access the target information belonging to an NSSAI the NF Service Consumer does not belong to.

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