**3GPP TSG-SA3 Meeting #99e *S3-201081-r26***

**e-meeting, 11 – 15 May 2020**

|  |
| --- |
| *CR-Form-v12.0* |
| **DRAFT CHANGE REQUEST** |
|  |
|  | **33.501** | **CR** |  - | **rev** | **-** | **Current version:** | **16.2.0** |  |
|  |
| *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:***  | Token-based authorization for indirect communication  |
|  |  |
| ***Source to WG:*** | CableLabs, Mavenir, Nokia, Nokia Bell Labs, Ericsson, Huawei, Hisilicon |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | 5G\_eSBA |  | ***Date:*** | 2020-04-30 |
|  |  |  |  |  |
| ***Category:*** | **B** |  | ***Release:*** | Rel-16 |
|  | *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-12 (Release 12)**Rel-13 (Release 13)Rel-14 (Release 14)Rel-15 (Release 15)Rel-16 (Release 16)* |
|  |  |
| ***Reason for change:*** | This draft-CR specifies token-based authorization for indirect communication. |
|  |  |
| ***Summary of change:*** | Define a token-based authorization for indirect communication. |
|  |  |
| ***Consequences if not approved:*** | Token-based authorization for Indirect communication not properly specified. |
|  |  |
| ***Clauses affected:*** | 13.3.0 (New), 13.4.1.X (new), 13.4.1.X.1 (new), 13.4.1.X.2 (new), 13.4.1.X.Y (new), 13.4.1.X.3 (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:*** |  |

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

#### 13.4.1.X Service access authorization in indirect communication scenarios

##### 13.4.1.X.1 General

Editor's Note: General introduction to be added.

##### 13.4.1.X.2 Authorization for indirect communication without delegated discovery procedure

###### 13.4.1.X.2.1 With mutual authentication between NF Service Consumer and NRF at the transport layer

This clause covers the scenario where the NF Service Consumer and the NRF are connected over a mutually authenticated TLS connection.



**Figure 13.4.1.X.2.1-1: Authorization and service invocation procedure, for indirect communication without delegated discovery, with mutual authentication between NF and NRF at the transport layer**

**Discovery of the NF Service Producer:**

1. Optionally, the NF Service Consumer may discover the NF Service Producer before requesting authorization to invoke the services of the NF Service Producer.

**NF Service Consumer authorization:**

 1-2.

After mutual authentication between NF Service Consumer and NRF at the transport layer, the NF Service Consumer and NRF perform the "Access token request before service access" procedure as described in clause 13.4.1.1. If the NF Service Consumer has already discovered the NF Service Producer, it can also perform the "Access token request for a specific NF Service Producer/NF Service Producer instance" procedure as described in clause 13.4.1.1.

**Service request:**

The NF Service Consumer, SCP, NRF and NF Service Producer perform the procedure "Indirect Communication without delegated discovery Procedure" described in clause 4.17.11 of TS 23.502 [8]. The following steps describe how the access token received from steps 1 and 2 is used in this procedure.

3. If no cached data is available, the NF Service Consumer discovers the NF Service Producer via the SCP.

4. The NF Service Consumer sends a service request for the specific service to the SCP. The service request includes the access token as received in step 2, and may include the NF Service Consumer client credentials assertion as defined in clause 13.3.8.

5. The SCP selects a NF Service Producer instance, performs the API root modifications and forwards the received request to the selected NF Service Producer instance. The request contains the access token and may contain the NF Service Consumer client credentials assertion if received in step 4.

6. To authorize the access, the NF Service Producer authenticates the service consumer NF using one of the methods described in clause 13.3.2.2 and if successful, it validates the access token as described in clause 13.4.1.1 by verifying the signature and checking if the requested service is part of the token's scope.

7. If the checks in step 6 are successful, the NF Service Producer processes the service request and provides a service response.

8. The SCP performs reverse API root modifications and forwards the service response.

###### 13.4.1.X.2.2 Without mutual authentication between NF and NRF at the transport layer

When there is no mutual authentication between NF Service Consumer and NRF at the transport layer, the NF Service Consumer performs the following procedure to obtain the access token from NRF and uses it for service access at the NF Service Producer. In this clause, the authentication of NF service consumer by the NRF and by the NF service producer is based on any of the methods described in clauses 13.3.1.2 and 13.3.2.2.



**Figure 13.4.1.X.2.2-1: Authorization and service invocation procedure, for indirect communication without delegated discovery, without mutual authentication between NF and NRF at the transport layer**

0. Optionally, the NF Service Consumer may discover the NF Service Producer before requesting authorization to invoke the services of the NF Service Producer.

1. The NF Service Consumer sends an access token request (Nnrf\_AccessToken\_Get Request) to the SCP with parameters as specified in 13.4.1.1. The access token request may additionally include the NF Service Consumer client credentials assertion as defined in clause 13.3.8.

2. The SCP forwards the access token request (Nnrf\_AccessToken\_Get Request) to the NRF. Th request may include the NF Service Consumer client credentials assertion if received in step 1.

3. The NRF authenticates the service consumer NF using one of the methods described in clause 13.3.2.2. If the NF Service Consumer authentication is successful and the NF Service Consumer is authorized based on the NRF policy, the NRF issues an access token as described in clause 13.4.1.1. The NRF uses the NF Service Consumer NF Instance ID as the subject of the access token.

4. The NRF sends the access token to the SCP in an access token response (Nnrf\_AccessToken\_Get Response).

5. The SCP forwards the access token response (Nnrf\_AccessToken\_Get Response) to the NF Service Consumer, including the access token.

6. The NF Service Consumer sends the service request to the SCP. The service request includes the access token received in Step 5 and may include the NF Service Consumer client credentials assertion,

7. The SCP forwards the service request to the NF Service Producer. The service request includes the access token received in step 6, and may include the NF Service Consumer client credentials assertion if received in step 6.

8. The NF Service Producer authenticates the NF service consumer by one of the methods described in clause 13.3.2.2 and if successful, it validates the access token as described in clause 13.4.1.1.

9, If the validation of the access token is successful, the NF Service Producer sends the service response to the SCP.

10. The SCP forwards the service response to the NF Service Consumer.

13.4.1.X.3 Authorization for indirect communication with delegated discovery procedure

This clause covers the scenario where the NF Service Consumer use the SCP to discover and select the NF Service Producer instance that can process the service request.



**Figure 13.4.1.X.3-1: Authorization and service invocation procedure, for indirect communication with delegated discovery,**

1. The NF Service Consumer sends a service request to the SCP. The service request may include the NF Service Consumer client credentials assertion as defined in clause 13.3.8.

2. The SCP may perform a service discovery with the NRF.

3. The SCP sends an access token request (Nnrf\_AccessToken\_Get Request) to the NRF. The access token request includes parameters as defined in clause 13.4.1.1. The access token request may include the NF Service Consumer client credentials assertion if received in Step 1.

4. The NRF authenticates the NF service consumer using one of the methods described in clause 13.3.2.2. If cNF authentication is successful and the NF Service Consumer is authorized based on the NRF policy, the NRF issues an access token as described in clause 13.4.1.1. The NRF uses the NF Service Consumer instance ID as the subject of the access token.

5. The NRF sends the access token to the SCP in an access token response (Nnrf\_AccessToken\_Get Response).

6. The SCP sends the service request to the NF Service Producer. The service request includes the access token received in Step 5, and may include the NF Service Consumer client credentials assertion if received in Step 1.

7. The NF Service Producer authenticates the NF service consumer by one of the methods described in clause 13.3.2.2 and if successful, it validates the access token as described in clause 13.4.1.1.

8. If the validation of the access token is successful, the NF Service Producer sends the service response to the SCP.

9. The SCP forwards the service response to the NF Service Consumer.

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