**3GPP TSG-SA3 Meeting #108e *S3-222028-r2***

**e-meeting, 22 - 26 August 2022**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **33.501** | **CR** | 1460 | **rev** | **-**  | **Current version:** | **16.11.0** |  |
|  |
| *For* ***[HE](http://www.3gpp.org/3G_Specs/CRs.htm%22%20%5Cl%20%22_blank)******[LP](http://www.3gpp.org/3G_Specs/CRs.htm%22%20%5Cl%20%22_blank)*** *on using this form: comprehensive instructions can be found at <http://www.3gpp.org/Change-Requests>.* |
|  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME |  | Radio Access Network |  | Core Network | **x** |

|  |
| --- |
|  |
| ***Title:***  | Adding optional use of CCA for delegated discovery |
|  |  |
| ***Source to WG:*** | China Telecom, Nokia, Nokia Shanghai Bell, Huawei, Mavenir |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** |  |  | ***Date:*** | 2022-08-22 |
|  |  |  |  |  |
| ***Category:*** | F |  | ***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-15 (Release 15)Rel-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)* |
|  |  |
| ***Reason for change:*** | According to the current procedure in subclause 13.4.1.3.2 TS33.501, the authentication between NF and NRF using CCA is missed in case of indirect communication with delegated discovery procedure. Having CCA in delegated discovery would have at least three benefits:1. If CCA is already sent during discovery and NRF is rejecting the discovery request, SCP would not send an access token request, but respond back to NFc with the rejection.
2. As per subclause 13.3.1.3 TS33.501, access token may be supported for discovery authorization. Thus, CCA could be used to prevent token replay attack.
3. Consider the situation where the Consumer is authorized to discover expected NF instance, while the SCP is not. With CCA, the SCP can show its intension to NRF that it is discovering the expected NF instance on behalf of the Consumer. Then the NRF can authorize the discovery request according to the type of the NF Service Consumer.
 |
|  |  |
| ***Summary of change:*** | Adding optional use of CCA during discovery as well so that the NRF may also be able to authenticate the NF Service Consumer using CCA. |
|  |  |
| ***Consequences if not approved:*** | The authentication between NF and NRF will be missed. |
|  |  |
| ***Clauses affected:*** | 13.4.1.3.2 |
|  |  |
|  | **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 the change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

##### 13.4.1.3.2 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 13.4.1.3.2-1: 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's CCA as defined in clause 13.3.8.The NF Service Consumer may include an access token in the service request if it has received an access token in a previous service response. If a previously received access token has expired, the NF Service Consumer may include discovery parameters as specified in TS 29.500 [74] clause 5.2.3.2.7 in the service request.

If the CCA is included, the NF type of the expected audience in the CCA shall contain both "NRF" and "NF Service Producer".

2. The SCP may perform a service discovery with the NRF. The service discovery request may include the NF Service Consumer's CCA if received in Step 1. If NF Service Consumer has included an access token in step 1, or if the SCP has a cached granted access token, then SCP may reuse the access token and proceeds to step 6.

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's CCA if received in Step 1.

4. The NRF authenticates the NF Service Consumer using one of the methods described in clause 13.3.1.2. If 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 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 an access token (i.e., received in Step 1, received in Step 5, or previously cached), and may include the NF Service Consumer's CCA 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. The SCP may include the access token in the service response to NF Service Consumer for possible re-use in subsequent service requests.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of the change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*