**3GPP TSG-SA3 Meeting #98e *S3-200286***

**e-meeting, 2 – 6 March 2020**

|  |
| --- |
| *CR-Form-v12.0* |
| **DRAFT CHANGE REQUEST** |
|  |
|  |  | **CR** |   | **rev** |  | **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:***  | Clarifications and corrections for token-based authorization in Scenario C |
|  |  |
| ***Source to WG:*** |  |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** |  |  | ***Date:*** |  |
|  |  |  |  |  |
| ***Category:*** |  |  | ***Release:*** |  |
|  | *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:*** | The proposed changes in this CR are on top of the approved draft-CR S3-194522.* Added text in the "General" clause
* Clarifications
* Corrections
 |
|  |  |
| ***Summary of change:*** |  |
|  |  |
| ***Consequences if not approved:*** |  |
|  |  |
| ***Clauses affected:*** | 13.4.1.X (new), 13.4.1.X.1 (new), 13.4.1.X.2 (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

Indirect communication scenarios are described in Annex E of TS 23.501 [2] and clauses 4.17.9, 4.17.10 and 4.17.11 of TS 23.502 [8]. Clause 13.4.1.X in the present specification describes token-based authorization using OAuth 2.0 for indirect communication scenarios, both with and without delegated discovery.

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

Figure 13.4.1.X.2-1: Authorization and service invocation procedure

**Discovery of the NF Service Producer:**

0. 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. 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 (Step 0), it can also perform the "Access token request for a specific NF Producer/NF Producer service instance" procedure as described in clause 13.4.1.1.

**Service request:**

The NF Service Consumer, SECOP, 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 in steps 1 and 2 is used in this procedure.

3. If the NF Service Consumer has not already discovered the NF Service Producer, the NF Service Consumer now performs service discovery of the NF Service Producer.

4. The NF Service Consumer sends a service request for the specific service to the SECOP. The service request includes the access token for the NF Service Producer providing the service as received in step 2.

5. The SECOP 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 token as received in step 4. and valid for the NF Service Consumer.

6. To authorize the access the NF Service Producer validates the token by verifying the signature and checking if the requested service is part of the token's scope. If the checks are ok the NF Service Producer processes the request and provides a response.

7. The SECOP performs revers API root modifications and forwards the response.

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