**3GPP TSG-SA3 Meeting #105-e *S3-*** ***214264-r3***

e-meeting, 8 - 19 November 2021

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  |  | **CR** | **DRAFT** | **rev** |  | **Current version:** | **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:*** | Authorization mechanisms for data consumer to access data from data producer via DCCF | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Nokia, Nokia Shanghai Bell, Lenovo, Motorola Mobility, Mavenir, Verizon, Ericsson, Huawei, HiSilicon, China mobile | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | eNA\_Ph2 | | | | |  | ***Date:*** | | | 2021-11-08 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | B |  | | | | | ***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-12 (Release 12)* *Rel-13 (Release 13) Rel-14 (Release 14) Rel-15 (Release 15) Rel-16 (Release 16)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | Rational for removing the Ed. Note – “Whether having two CCA is required and if needed how to solve transferring two CCAs (when applicable) is FFS.”  In the case when SCP is in between DCCF and NRF (or NFp) then DCCF may optionally also send CCA\_DCCF along with the CCA\_NWDAF. CCA\_DCCF even though optionally present is not required for the fulfillment of this solution. Therefore, the solution only requires one CCA (i.e. CCA\_NWDAF) to be sent. In case both the CCAs are sent (i.e CCA\_NWDAF and CCA\_DCCF), the transfer of two CCA(s) will be specified in stage 3.  Further in order to remove the Ed. Note – “Whether a single access token is required and the compatibility with Rel 15,16, NRF and NF Service Producer is FFS.” , appropriate changes are proposed and clarifications are provided. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Adding the authorization aspects for data consumer to access data via DCCF as agreed in the Solution 10 of TR 33.866 | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | No removal of Ed Notes for security procedure for eNA Rel-17 feature | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | New Annex | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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 Change 1 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

X.2 Authorization of NF Service Consumers for data access via DCCF

The detailed procedure for NF Service Consumer to receive data from Service Producers via DCCF is depicted in Figure X.2-1:



Figure X.2-1: Service Consumer Authorization to receive data from Service Producers via DCCF

1-3. NF Service Consumer shall send a request to the NRF to receive an access token to request services of DCCF. NRF after verifying shall generate access token and sends it to the NF Service Consumer.

4. The NF Service Consumer initiates a NF service request to the DCCF which includes the access\_token\_nwdaf. The NF Service Consumer shall also generate a Client Credentials Assertion (CCA) token (CCA\_NWDAF) as described in the clause 13.3.8 and include it in the request message in order to authenticate itself towards the NF Service Producers.

NOTE: The procedure of NF Service Consumer (e.g. NWDAF) requesting the services provided by NF Service Producer via DCCF is defined in Clause 6.2.6.3 of TS 23.288[x].

5. The DCCF shall verify if the access\_token\_nwdaf is valid and executes the service.

6. The DCCF determines the NF Service Producer(s) from where the data is to be collected (as specified in Clause 6.2.6.3.2 in TS 23.288[x]).

NOTE: If the NF Service Consumer sends the NF Service Producer information (i.e. NF Service Producer type and Instance ID) along with the service request in Step 4, then DCCF does not determine the NF Service Producer, but requests an access token from the NRF using the NF Producer details sent by the NF Service Consumer (as described in Step 7.)

7. The DCCF sends a Nnrf\_AccessToken\_Get request to NRF including the information to identify the target NF (NF Service Producer), the source NF (NF Service Consumer e.g. NWDAF), the NF Instance ID of DCCF and the CCA\_NWDAF provided by the NF Service Consumer.

NOTE: The NF Instance ID of DCCF is included in a different IE than source NF so that Rel-16 NRF will ignore the new IE.

8. The NRF shall check whether the DCCF and the NF Service Consumer (e.g. NWDAF) are allowed to access the service provided by the identified NF Service Producers. NRF authenticates both DCCF and NWDAF based on one of the SBA methods described in clause 13.3.1.2. DCCF may include an additional CCA for authentication.

NOTE: Rel-16 or earlier NRF takes CCA to authenticate NF Service Consumer if available (i.e., authentication is not based on TLS).

NOTE: In the case the NRF is from Rel-16 or earlier, after the NRF receives Nnrf\_AccessToken\_Get request, the NRF validates whether the NF Service Consumer (e.g., NWDAF) is authorized to receive the requested service from the NF Service Producer. The NRF from Rel-16 or earlier does not validate whether the DCCF is authorized to receive the requested service.

9. The NRF after successful verification then generates and provides an access token to the DCCF as described in the clause 13.4.1.1.2, with NF Service Consumer Instance (subject), and an additional access token claim containing the identity of DCCF, in order to authorize both NF Service Consumer (i.e. NWDAF) and DCCF to consume the services of NF Service Producer.

NOTE: In the case the NRF is from Rel-16 or earlier, the NRF generates an OAuth2.0 access token with “subject” claim mapped to the NF Service Consumer (e.g., NWDAF) and no additional claim for the DCCF identity is added.

10. The DCCF requests service from the NF Service Producer. The request also consists of CCA\_NWDAF, so that the NF Service Producer(s) authenticates the NF Service Consumer (e.g. NWDAF).

11. The NF Service Producer(s) authenticate the NF Service Consumer and verify the access token as specified in the Clause 13.4.1.1.2 and ensures that the DCCF identity is included as an access token additional claim. If the DCCF identity is not included in the access token additional claims, e.g., NRF is Release 16 or prior, the NF Service Producer shall authorize the DCCF locally. After authentication and authorization is successful, the NF Service Producer(s) execute the service after successful verification. DCCF may include an additional CCA for authentication.

NOTE: Rel-16 or earlier NF Service Producer takes CCA to authenticate NF Service Consumer if available (i.e., authentication is not based on TLS).

12. The NF Service Producer(s) shall provide requested data to the DCCF.

13. The DCCF forwards the received data to the data consumer(s).

NOTE: In the case a new data consumer comes at a later stage to request the data, which is already being collected by DCCF, steps 1-10 apply. When the request is received by the NF Service Producer (i.e. the data producer), it authenticates the NF Service Consumer and verifies the access token provided along with the service request and sends to DCCF the access token verification response. DCCF based upon the response received, either updates the subscription info to include the new data consumer as well and sends the data to both the consumers (as specified in Clause 6.2.6.3.2 in TS 23.288[x]), or in the case of access token verification failure, the DCCF rejects the request received by the data consumer.

NOTE: In the case the NF Service Producer is from Rel 16 or earlier, the NF Service Producer authorizes the NF Service Consumer (e.g., NWDAF) by validating the received OAuth2.0 access token which has the “subject” claim maps to the NF Service Consumer (e.g., NWDAF). Rel-16 or earlier NF Service Producer authorization of the DCCF is a deployment specific based on any of the available 5GC authorization method(s).

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of Change 1 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*