**3GPP TSG-SA3 Meeting SA3#110-adhoc-e *draft\_S3-231980-r1***

**Electronic meeting, 17 - 21 April 2023**

|  |
| --- |
| *CR-Form-v12.1* |
| **DRAFT CHANGE REQUEST** |
|  |
|  | **33.501** | **CR** | **draft-CR** | **rev** | **-** | **Current version:** | **18.1.0** |  |
|  |
| *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:***  |  Skeleton for Security aspects of enablers for Network Automation for 5G - phase 3 |
|  |  |
| ***Source to WG:*** | China mobile |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | eNA\_Ph3 |  | ***Date:*** | 2023-04-10 |
|  |  |  |  |  |
| ***Category:*** | B |  | ***Release:*** | Rel-18 |
|  | *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:*** |  |
|  |  |
| ***Summary of change:*** | Skeleton for how the work on the eNA phase 3 security study can be included in TS 33.501. |
|  |  |
| ***Consequences if not approved:*** |  |
|  |  |
| ***Clauses affected:*** |  |
|  |  |
|  | **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:*** |  |

\*\*\* BEGIN CHANGES \*\*\*

Annex X (normative):
Security aspects of enablers for Network Automation (eNA) for the 5G system (5GS)

# X.1 General

This Annex provides security requirements and procedures for the Network Automation features.

The feature for enablers for Network Automation by 5GS is described in 3GPP TS23.501[2] and 3GPP TS23.288 [105].

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: NF Service Consumer Authorization to receive data from NF 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, to be used for data collection request. 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 0: 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 [105].

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[105]).

NOTE 1: 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 Service 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 1a: 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 , and the DCCF as the proxy is allowed to request the service from the identified NF Service Producers on behalf the NF Service Consumer. 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 2: A Rel-16 NRF takes CCA to authenticate NF Service Consumer if available (i.e., authentication is not based on TLS).

NOTE 3: 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 (e.g.. NWDAF) and DCCF to consume the services of NF Service Producer.

NOTE 4: 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) assure that the DCCF as the proxy is allowed to receive the response message on behalf the NF Service Consumer, and execute the service after successful verification. DCCF may include an additional CCA for authentication.

NOTE 5: Rel-16 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 NF Service Consumer(s).

NOTE 6: In the case a new NF Service 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 newNF Service Consumer as well and sends the data to both the consumers (as specified in Clause 6.2.6.3.2 in TS 23.288 [105]), or in the case of access token verification failure, the DCCF rejects the request received by the NF Service Consumer.

NOTE 7: 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).

X.3 Authorization of NF Service Consumers for data access via DCCF when notification sent via MFAF

The detailed procedure for NF Service Consumer to receive data from Service Producers via DCCF when notification is sent via MFAF is depicted in Figure X.3-1:



Figure X.3-1: Service Consumer Authorization to receive data from Service Producers via MFAF

Steps 1-9 are same as Steps 1 – 9 of Annex X.2

10-11. The DCCF sends an access token request to the NRF to request service from MFAF. NRF after verifying sends access\_token\_dccf to DCCF to consume the services of MFAF.

12. DCCF shall then send the Nmfaf\_3daDataManagement\_Configure request to MFAF (as specified in the Clause 6.2.6.3.2 in TS 23.288[105]) along with the access\_token\_dccf.

Steps 13 – 14 are same as Steps 10 – 11 of Annex X.2

15. The NF Service Producer(s) shall provide requested data to the MFAF.

16. The MFAF forwards the received data to the data consumer(s).

NOTE 1: In the case a new data consumer comes at a later stage to request the data, which is already being collected by DCCF, steps 1-9 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 at the MFAF to include the new data consumer as well and MFAF sends the data to both the consumers (as specified in Clause 6.2.6.3.2 in TS 23.288 [105]), or in the case of access token verification failure, the DCCF rejects the request received by the data consumer and does not update the subscription at the MFAF.

NOTE 2: 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).

X.4 Security protection of data via Messaging Framework

The transfer of the data between the data source and data consumer via the messaging framework shall be confidentiality, integrity, and replay protected.

Confidentiality protection, integrity protection, and replay-protection shall be supported on the new interfaces between 3GPP entities and MFAF by reusing the existing security mechanism defined for SBA in Clause 13.

X.5 Protection of data transferred between AF and NWDAF

As specified in TS 23.288[105], the NWDAF may interact with an AF to collect data from UE Application(s) as an input for analytics generation. The AF can be in the MNO domain or an AF external to MNO domain. To enhance the 5GS to support collection and utilisation of UE related data for providing the inputs to generate analytics information (to be consumed by other NFs), the communication between AF and NWDAF needs to be secured.

The NWDAF interacts with the 5GC NFs and the AF using Service-based Interfaces. The existing 5G security mechanism can be reused for the transfer of UE data over the SBA interface between AF and NWDAF. When the AF is located in the operator’s network, the NWDAF uses Service-Based Interface as depicted in clause 13 to communicate with the AF directly. When the AF is located outside the operator’s network, the NEF is used to exchange the messages between the AF and the NWDAF. The security aspects of NEF is specified in clause 12.

X.6 Protection of UE data in transit between NFs

According to clause 13.1.0, all network functions shall support mutually authenticated TLS and HTTPS. TLS shall be used for transport protection within a PLMN unless network security is provided by other means. Thus, communication between NFs is integrity, confidentiality and replay protected.

NFs shall obtain an access token from NRF for requesting analytics from an analytics function or providing analytics data to the analytics function.

# X.7 User consent requirements

The user consent requirements for enablers of network automation shall comply with Annex V of the present document and TS 23.288 [105].

# X.a Protection of data and analytics exchange in roaming case

Editor’s Note: This clause captures the protection of data and analytics exchange in roaming case.

# X.b Authorization of selection of participant NWDAF instances in the Federated Learning group

Editor’s Note: This clause captures the authorization of selection of participant NWDAF instances in the Federated Learning group.

# X.c Security for AI/ML model storage and sharing

Editor’s Note: This clause captures the security for AI/ML model storage and sharing.

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