3GPP TSG-SA3 Meeting #115 S3-240913-r1

Athens, Greece, 26 February -01 March 2024

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.501** | **CR** | **1921** | **rev** |  | **Current version:** | **18.4.0** |  |
|  | | | | | | | | |
| *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:*** | Correct procedure for authorization of selection of participant NWDAF instances in the Federated Learning group | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Huawei, HiSilicon | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | eNA\_Ph3\_SEC | | | | |  | ***Date:*** | | | 2024-02-18 |
|  |  | | | |  | |  | | |  |
| ***Category:*** |  |  | | | | | ***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 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-15 (Release 15) Rel-16 (Release 16) Rel-17 (Release 17) Rel-18 (Release 18)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | This proposal is to correct procedure for authorization of selection of participant NWDAF instances in the Federated Learning group.  As description in clause 6.2C.2.2, TS 23.288,  *Then the FL client NWDAF(s) terminate the local model training and if the final aggregated ML model information is received from the FL server NWDAF, the FL client NWDAF(s) can store it for further use.*  The FL server may send the globally optimal ML model information to the consuer, in other words, the FL client can get the global model from the FL Server. However, the NWDAF FL client may not register its vendor ID in the NRF, and the FL server NWDAF couldn’t check whether the FL client is authorzied to get the gloable model.  If the NRF doesn’t check model access right of the FL clients, the FL server may send the gloable model to the FL client who’s vendor ID is not the Interoperability indicator. As the result, the Federated Learning group’s ML model may leak out to the unauthorized client NWDAF. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | It is proposed to make NRF checks the permission of the FL client obtaining the FL server model. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | The Federated Learning group’s ML model may leak out to the unauthorized client NWDAF. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | X.9 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | |  | | | | | | | | |

# X.9 Authorization of selection of participant NWDAF instances in the Federated Learning group

The authorization for selecting participant NWDAF instances in the Federated Learning (FL) group uses token-based authorization as specified in clause 13.4.1, with the following additions.

Figure X.9-1 depicts the authorization mechanism for NWDAF containing MTLF acting as FL Server to initiate the Federated Learning process on the NWDAF containing MTLF(s) acting as FL Client(s). The authorization is based upon the FL capability type (FL server or FL client) provided by the NWDAF containing MTLF acting as FL server during registration, and the Analytics ID and Interoperability Indicator per Analytics ID provided by the NWDAF containing MTLF acting as FL client during registration.

Editor’s note: The use of Service area and Availability time requirement for authorization is FFS.



Figure X.9-1: FL Authorization for selecting participant NWDAF instances

Step 1a. The NWDAF containing MTLF acting as FL client registers to the NRF with its FL related information, including Vendor ID, supported FL capability (FL client), Analytics ID(s) and Interoperability Indicator per Analytics ID as described in clause 5.2 of TS 23.288.

Step 1b. The NWDAF containing MTLF acting as FL server registers to the NRF with its Vendor ID, FL capability (FL Server) and Interoperability Indicator per Analytics ID as described in clause 5.2 of TS 23.288.

Step 2. The NWDAF containing MTLF acting as FL server (NF Service Consumer) sends a discovery request to NRF and receives the available NWDAFs containing MTLF acting as FL client(s) (NF Service Producer) as a response, as specified in clause 6.2C.2.1 of TS 23.288 [105].

Step 3. The NWDAF containing MTLF acting as FL server (NF Service Consumer) sends an access token request to the NRF as specified in clause 13.4.1. The access token request may contain the Analytics ID for the requested Federated Learning process.

Step 4. The NRF authorizes the NWDAF containing MTLF acting as FL server (NF Consumer) based upon the information received in Step 1b, and after verifying that the Server NWDAF’s Vendor ID is included in the Interoperability Indicator provided in Step 1a for the requested Analytics ID If the authorization succeeds, NRF generates the access token(s) as specified in clause 13.4.1. The access token claims may include the Analytics ID for the request Federated Learning process.

The NRF also needs to verify the Client NWDAF’s Vendor ID is included in the Interoperability Indicator provided in Step 1b for the requested Analytics ID before generating the access token(s).

NOTE: Fine-grained authorization can be done locally at the NWDAFs containing MTLF acting as FL client(s) (NF Service Producer).

Step 5a, 5b. The NRF sends the access token to the NWDAF containing MTLF acting as FL Server, or rejects the request in case of failed authorization, as described in clause 13.4.1.

Step 6. The NWDAF containing MTLF acting as FL server sends the service request to the NWDAF(s) containing MTLF acting as FL client with the access token received in Step 5a. along with the Analytics ID information for which the FL process is to be performed, as described in TS 23.288 [105].

Step 7, 8. The NWDAF containing MTLF acting as FL client (NF Service Producer) verifies the received access token as specified in clause 13.4.1. In case of successful access token verification, the NWDAF containing MTLF acting as FL client sends a success response to the NWDAF containing MTLF acting as FL server, as described in TS 23.288 [105].

Step 9. After a successful response from the NWDAF(s) containing MTLF acting as FL client, the NWDAF containing MTLF acting as FL server initiates the Federated Learning process as described in TS 23.288 [105].

Authorization of the NWDAF containing MTLF acting as FL client is implicit, since it can join a Federated Learning group only when selected by the NWDAF containing MTLF acting as FL server.