**3GPP TSG-SA3 Meeting #109-AdHoc *draft-S3-230209-r1***

**e-meeting. 16th January – 20th January 2023**

**Source: Intel**

**Title: FL GROUP AUTHORIZATION OF NWDAF(S) IN 5GC**

**Document for: Approval**

**Agenda Item: 5.8**

# 1 Decision/action requested

***This pCR adds a solution to TR 33.738. It is requested to approve this pCR for TR 33.738.***

# 2 References

# 3 Rationale

*This solution addresses Key Issue #2 (Authorization of selection of participant NWDAF instances in the Federated Learning group). The proposed solutions use existing SBA architecture for token-based authorization.* *NWDAF MTLF (FL Server) can select which Federated Learning task it wants to create by verifying the access token presented by the NWDAF AnLF. NWDAF MTLF (FL Client) can select which Federated Learning group it wants to join by verifying the access token presented by the NWDAF MTLF (FL Server).*

# 4 Detailed proposal

SA3 is kindly requested to agree on the pCR below to TR 33.738

\*\*\*\*\*Start of Changes\*\*\*\*\*

6.Y Solution #Y: FL GROUP AUTHORIZATION OF NWDAF(S) IN 5GC

6.Y.1 Introduction

This solution addresses Key Issue #2 (Authorization of selection of participant NWDAF instances in the Federated Learning group). The proposed solutions use existing SBA architecture for token-based authorization.

6.Y.2 Solution details

The detailed procedure for NWDAF AnLF/NWDAF MTLF (FL Server) to get token from NRF and receive services from NWDAF MTLF (FL Server)/NWDAF MTLF (FL Client) is depicted in Figure 6.Y.2-1



**Figure 6.Y.2-1 NWDAF AnLF/NWDAF MTLF (FL Server) Authorization to receive services from NWDAF MTLF (FL Server)/NWDAF MTLF (FL Client)**

NOTE: Steps 1 to 4 are not specific to FL scenario but details existing mechanisms. Step 5 to 13 are related to FL scenario.

0. NWDAF registers with NRF. If NWDAF MTLF as FL server determines ML model requires FL, the FL Server discovers and selects other NWDAF(s) MTLF as FL Client(s) from NRF. If NWDAF MTLF without FL server capability determines ML model requires FL, the MTLF discovers and selects FL sever from NRF.

1-3. NF(NWDAF AnLF or MTLF) Service Consumer sends a request to the NRF to receive an access token to request NWDAF MTLF (FL Server) services. NRF, after verifying, generates an access token and sends it to the NF(NWDAF ANLF OR MTLF) Service Consumer. Access tokens contain NWDAF MTLF (FL Server specific token).

4. The NF(NWDAF AnLF OR MTLF) Service Consumer initiates an NF service request to the NWDAF MTLF (FL Server), which includes the access\_token\_nwdaf. The NF(NWDAF AnLF OR MTLF) Service Consumer also generates a Client Credentials Assertion (CCA) token (CCA\_NWDAF) and includes it in the request message to authenticate itself towards the NF Service Producers.

5. The NWDAF MTLF (FL Server) verifies if the access\_token\_nwdaf is valid and starts FL group.

6. If The NWDAF MTLF (FL Server) determines to start the FL group for analytics id, The NWDAF MTLF (FL Server) sends a Nnrf\_AccessToken\_Get request to NRF including the information to identify the target NF (NWDAF MTLF (FL Client)), the source NF (NWDAF AnLF OR MTLF) Service Consumer, the NF Instance ID of NWDAF MTLF (FL Server) , Analytics ID, FL local model training service type, FL group ID and the CCA\_NWDAF provided by the NF(NWDAF AnLF OR MTLF) Service Consumer.

7. The NRF checks whether the NWDAF MTLF (FL Server) and the NF(NWDAF ANLF OR MTLF) Service Consumer (e.g. NWDAF) are allowed to access the service provided by the identified NF Service Producers(NWDAF MTLF (FL Client)) for the given Analytics ID included in step 6, and the NWDAF MTLF (FL Server). NRF authenticates both NWDAF MTLF (FL Server) and NWDAF(FL consumer, e.g., AnLF) based on one of the SBA methods described in clause 13.3.1.2 of TS 33.501. NWDAF MTLF (FL Server) may include an additional CCA for authentication.

8. The NRF, after successful verification, then generates and provides an access token to the NWDAF MTLF (FL Server); the claims in the token include the NF Instance Id of NRF (issuer), NF Instance Id of the NF Service Consumer (subject), NF type of the NF Service Producer (audience), expected service name(s), (scope), expiration time (expiration), FL group ID, Analytics ID(s), ML model ID(s) and optionally "additional scope" information (allowed resources and allowed actions (service operations) on the resources), with NF(NWDAF AnLF OR MTLF) Service Consumer Instance (subject), to authorize both NF(NWDAF AnLF OR MTLF) Service Consumer (e.g.. NWDAF) and NWDAF MTLF (FL Server) to consume the services of NWDAF MTLF (FL Client).

Editor’s Note: Use of Model ID, FL group id is FFS and based on SA2’s conclusions.

9. NWDAF MTLF (FL Server) finalize the FL group with NWDAF MTLF (FL Client) selected from the list received from NRF.

10. The NWDAF MTLF (FL Server) requests service (local model updates) from the NWDAF MTLF (FL Client). The request also consists of CCA\_NWDAF so that the NF Service Producer(s) authenticates the NF(NWDAF ANLF OR MTLF) Service Consumer (e.g., NWDAF).

11. The NWDAF MTLF(s) (FL client) authenticates the NF(NWDAF AnLF OR MTLF) Service Consumer and verifies the access token, and ensures that the NWDAF MTLF (FL Server) identity, FL group ID, Analytics ID(s), ML model ID(s) is included as an access token additional claim.

12. The NWDAF MTLF(s) (FL client) provides requested data to the NWDAF MTLF (FL Server). Global Model updates/aggregation is done at NWDAF MTLF (FL Server).

13. NWDAF MTLF (FL Server) feedback on the NF Service Response.

### 6.Y.3 Evaluation

This solution reuses the existing 5GS security mechanisms, including the current SBA security mechanisms.

NWDAF MTLF (FL Server) can select which Federated Learning task it wants to create by verifying the access token presented by the NWDAF AnLF. NWDAF MTLF (FL Client) can select which Federated Learning group it wants to join by verifying the access token presented by the NWDAF MTLF (FL Server). The solution fulfils the following requirements of KI 1.2:

Authorization of selection of participant NWDAF instances in the Federated Learning group shall be supported:

A server NWDAF shall be authorized to include a client NWDAF in a Federated Learning group. A client NWDAF shall be authorized to join a Federated Learning group.

Editor’s Note: Further Evaluation is FFS.

\*\*\*\*\*End of Changes\*\*\*\*\*