**3GPP TSG-SA3 Meeting #109AdHoc-e *draft\_S3-230239-r3***

**Electronic meeting, 16 - 20 January 2023**

**Source: Ericsson**

**Title: New solution for KI#2 to support authorization of participant NWDAFs in FL**

**Document for: Approval**

**Agenda Item: 5.8**

# 1 Decision/action requested

***It is requested to approve this proposal in TR 33.738 [1].***

2 References

[1] 3GPP TR 33.738 V0.4.0 "Study on security aspects of enablers for Network Automation for 5G - phase 3"

[2] 3GPP TR 23.700-81 V18.0.0 " Study of Enablers for Network Automation for 5G System (5GS); Phase 3"

# 3 Rationale

As per SA2 conclusion of "KI #8: Supporting Federated Learning in 5GC" in TR 23.700-81[2], the NWDAF containing MTLF as FL server triggers discovery and selection of NWDAF(s) containing MTLF as FL Client(s) to initiate the FL procedure. On the other hand, FL clients can also join an ongoing FL procedure dynamically during FLexecution phase.

This paper proposes a solution to address KI#2 for authorization of participant NWDAFs for FL procedure.

# 4 Detailed proposal

**\*\*\*\*** START OF 1st CHANGE **\*\*\*\***

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 23.501: "System Architecture for the 5G System; Stage 2".

[3] 3GPP TS 23.502: "Procedures for the 5G system, Stage 2".

[4] 3GPP TS 23.503: "Policy and Charging Control Framework for the 5G System".

[5] 3GPP TS 23.288: "Architecture enhancements for 5G System (5GS) to support network data analytics services".

[6] 3GPP TR 23.700-81: " Study of Enablers for Network Automation for 5G System (5GS); Phase 3".

[7] 3GPP TS 33.501: "Security architecture and procedures for 5G System".

[8] 3GPP TS 29.510: "Network function repository services; Stage 3".

[9] 3GPP TS 28.552: "5G performance measurements"

[XX] 3GPP TR 33.875: "Study on enhanced security aspects of the 5G Service Based Architecture (SBA)"

[x] <doctype> <#>[ ([up to and including]{yyyy[-mm]|V<a[.b[.c]]>}[onwards])]: "<Title>".

**\*\*\*\*** END OF 1st CHANGE **\*\*\*\***

\*\*\*\* START OF 2nd CHANGE \*\*\*\*

## 6.X Solution #X: Authorization of FL Server and FL Client in FL group

### 6.X.1 Introduction

This solution addresses Key issue #2: Authorization of selection of participant NWDAF instances in the Federated Learning group.

As per KI#2, both server NWDAF and client NWDAF shall be authorized for FL procedure.

- A server NWDAF shall be authorized to include a client NWDAF into a Federated Learning group.

- A client NWDAF shall be authorized to join a Federated Learning group.

For initiation of FL procedure or reselection of FL client(s) into a FL procedure, the server NWDAF triggers discovery and selection of NWDAF(s) and sends FL request to the client NWDAF.

* At the client NWDAF side, authorization of the server NWDAF that it can include the client NWDAF into the FL group can be achieved by reusing existing SBA token-based authorization upon receiving FL request.
* At the server NWDAF side, authorization of the client NWDAF to be included into a FL group is implicitly achieved as the server NWDAF only triggers the selection of FL client(s) into the FL group that it authorizes to be included.

This solution also considers interoperatiliy of different vendors of Server and Client NWDAF(s).

### 6.X.2 Solution details

Figure 6.X.2-1 illustrates the high-level procedure of the proposed solution.



Figure 6.X.2-1: High-level procedure for authorization of FL Server and FL Client in FL group

0. NWDAF containing MTLF as FL server or FL clients register to NRF with their FL related information, including Analytics ID(s), Interoperability ID, Vendor ID, Address information, FL capability Type (i.e. FL server or FL client), and Service Area etc.

NOTE: The Interoperability indicator indicates a list of NWDAF providers (vendors) that are allowed to retrieve ML models from the NWDAF containing MTLF.

Assumption: The NRF can verify the Vendor ID of the NWDAFs containing MTLF.

Editor's Note: How the NRF verifies the Vendor ID of the NFDAF is pending the resolution of Key Issue #11 NRF validation of NFc for access token requests in TR 33.875 "Study on enhanced security aspects of the 5G Service Based Architecture (SBA)"

1. The Server NWDAF discovers Client NWDAFs from NRF based on FL selection criteria e.g. Federated Learning capability, Interoperability ID, Analytics ID, etc.

Server NWDAF requests tokens for each of selected Client NWDAFs from NRF, with Analytics ID, Vendor ID and FL capability included in the request.

NRF verifies that the Server NWDAF's Vendor ID is included in the Client NWDAF's Interoperability ID for the Analytics ID and grants the token, based the information provided in Client NWDAF's NF profile.

2. The Server NWDAF sends FL request to the Client NWDAF(s) with the obtained token.

3. Each Client NWDAF checks whether the server NWDAF is authorized based on the token and decides whether to join the FL group.

4. The Client NWDAF(s) sends the response to the Server NWDAF.

5. The FL group is formed.

6. The Server NWDAF registers or updates its registration into NRF about the created FL Group with the following parameters: Federated Learning (FL) Correlation ID. the associated Analytics ID, Interoperability ID, allowed requester NF type or NF instance ID (e.g. NWDAF containing MTLF), allowed FL capability (e.g. FL client) etc.

If the Server NWDAF is about to reselect new Client NWDAF(s) into the FL group during FL execution phase, the Server can either trigger selection procedure again as step 1 to step 4 or receive notification from NRF and select new Client NWDAF(s) available as step 7 to step 9.

7-8. The Server NWDAF gets the information of the new Client NWDAF(s) via notifications from NRF.

9. The Server NWDAF requests tokens for each of selected Client NWDAFs from NRF as step1 and triggers the procedure as step 2-4.

6.3.3 Evaluation

This solution resolves Key Issue #2: Authorization of selection of participant NWDAF instances in the Federated Learning group.

This solution proposes to reuse existing SBA token-based authorization for authorization of server NWDAF and client NWDAF for FL procedures.

For initiation of a FL procedure or reselection of FL client(s) into a FL group, the server NWDAF requests token from NRF for each selected client NWDAF, to be authorized to include a client NWDAF into a FL group.

This solution also proposes that FL model sharing is authorized based on the Interoperability ID. When the server NWDAF requests token from NRF to include a client NWDAF into a FL group, NRF verifies that the server NWDAF's vendor ID is included in the client NWDAF's Interoperability ID and grants the token based the information provided in client NWDAF's NF profile.

In this solution, authorization is granted with NWDAF vendor granularity, but not for specific NF instances.

Editor's Note: Further evaluation is ffs.

\*\*\*\* END OF 2nd CHANGE \*\*\*\*