**3GPP TSG-SA3 Meeting #116 *draft\_S3-242588\_r2***

Jeju, South Korea, 20th - 24th May 2024 *Revision of S3-242160*

**Source: Ericsson**

**Title: New Solution to KI#2: Authorization of VFL participant involving NWDAF and AF**

**Document for: Approval**

**Agenda Item: 5.13**

# 1 Decision/action requested

***Approve the pCR to TR 33.784 [2] below.***

# 2 References

[1] TR 23700-84 V0.3.0 Study on Core Network Enhanced Support for Artificial Intelligence (AI)/Machine Learning (ML)

[2] TR 33.784 V0.1.0 Study on security aspects of Core Network Enhanced Support for AIML

[3] TS 33.501 V18.5.0 Security architecture and procedures for 5G System

# 3 Rationale

This contribution proposes a solution to KI#2 "Authorization mechanism of selection of VFL participants in the VFL group " using authentication and token-based authorization already specified in TS 33.501[3].

# 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 TR 38.843: "Study on Artificial Intelligence (AI)/Machine Learning (ML) for NR air interface".

[3] 3GPP TR 23.700-84: "Study on Core Network Enhanced Support for Artificial Intelligence (AI)/Machine Learning (ML)".

[4] RP-234039: “New WID on Artificial Intelligence (AI)/Machine Learning (ML) for NR Air Interface”.

[5] 3GPP TS 33.501: “Security architecture and procedures for 5G system”.

[6] "IEEE Guide for Architectural Framework and Application of Federated Machine Learning," in IEEE Std 3652.1-2020.3

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

 **\*\*\*\*** End of 1st CHANGE **\*\*\*\***

**\*\*\*\*** START of 2nd CHANGE **\*\*\*\***

## 6.Y Solution #Y: Authorization of VFL participants involving NWDAF and AF for External AF acting as FL server

### 6.Y.1 Introduction

This solution addresses Key Issue #2 "Authorization mechanism of selection of VFL participants in the VFL group" for the case External AF acting as FL server.

In this solution, the FL Server with VFL capability refers to the NWDAF/External AF that plays the role of the VFL Coordinator and/or active VFL participant, while the FL Client with VFL Capabilities refers to the NWDAF/External AF that plays the role of passive VFL participant.

The NRF is used as the authorization entity for the participation of VFL procedure.

When the External AF assumes the role of the VFL server, NEF registers to the NRF with the AF (VFL server) specific information (e.g., AF ID, AF provider/Vendor ID, Application ID, AF service ID) and its FL capability (VFL server) on behalf of the External AF. The NWDAF (VFL client) registers to the NRF with its FL capability (VFL client) and the authorization information used for VFL procedure, e.g., allowed VFL server (External AF) related information (AF ID, AF provider/Vendor ID, Application ID, AF service ID).

The NRF then authorizes the VFL service request for the VFL participants involving NWDAF and External AF based on the registered NEF/AF and NWDAF information.

Editor's Note: It is FFS whether additional information is needed for authorization of VFL participants involving NWDAF and External AF.

### 6.Y.2 Solution details



Figure 6.Y.2-1: VFL authorization when the External AF acts as a FL Server with VFL capabilities

Step 1a. The NWDAF containing MTLF acting as FL client registers to the NRF with its FL related information, including supported FL capability (FL client), Analytics ID(s) and Interoperability Indicator per Analytics ID as described in clause 5.2 of TS 23.288[x]. In addition, the FL client includes the authorization information used for VFL. It can be a list of AF specific information (e.g., AF ID, AF provider/Vendor ID, Application ID, AF service ID) that are allowed for VFL.

Step 1b. The External AF sends registration request to the NEF to indicate that it wants to create a VFL group by assuming the role of VFL server. In this request the external AF also sends information that can be used in the VFL participation decision such as Analytics ID, AF specific information (e.g., AF ID, AF provider/Vendor ID, Application ID, AF service ID), information about the data and data type that is available at AF etc.

NOTE: External AF may register its data via OAM configuration at NEF.

Step 1c. The NEF registers the External AF to the NRF with its FL related information, including supported FL capability (VFL server), Analytics ID(s), AF specific information (e.g., AF ID, AF provider/Vendor ID, Application ID, AF service ID), information about the data and data type available at the AF.

Editor's Note: The detailed parameters which need to be registered in the NRF are ffs. The definition about FL capability, data type, are ffs.

Step 2a, 2b. The External AF acting as FL server sends a discovery request to NRF via NEF and receives the available NWDAFs containing MTLF acting as FL client(s) as a response. The NEF enables this discovery procedure after authenticating and authorizing the AF.

Editor's Note: Whether the NF instance ID of NWDAF containing MTLF is sent to external AF is ffs.

Step 3a. The External AF acting as FL server sends the VFL service request (e.g., VFL preparation, sample alignment, feature alignment, VFL training, VFL inference) towards the NEF.

Step 3b. The NEF authorizes the External AF can trigger VFL service request towards NEF. The authentication and authorization between the NEF and the External AF acting as FL server can be performed as specified in TS 33.501[5] clause 12. If External AF is authorized, the NEF sends an access token request to the NRF to request the access token for the External AF acting as FL server to perform VFL service request towards the FL clients. The token request may contain the Analytics ID for the requested VFL process and also AF specific information (e.g., AF ID, AF provider/Vendor ID, Application ID, AF service ID).

Step 4. NRF checks whether the NF Service consumer (NEF) is authorized to access the requested service in FL client (NWDAF). In case of the NF Service Consumer (NEF) request VFL service for the External AF acting as FL server, the NRF also verifies that the AF specific information (e.g., AF ID, AF provider/Vendor ID, Application ID, AF service ID) is included in the authorization information used for VFL provided by the FL client in Step 1a. If the authorization succeeds, NRF generates the access token(s) as specified in TS 33.501[5] clause 13.4.1. The access token claims may include the Analytics ID for the request Federated Learning process. The access tokens are generated for the NEF (e.g., NEF as subject). The access token claims may include the AF specific information (e.g. AF ID, AF provider/Vendor ID, Application ID, AF service ID) .g. AF acting FL service is as service consumer .

NOTE: Fine-grained authorization can be done locally at the NWDAFs containing MTLF acting as FL client(s). Also, fine-grained authorization can be done locally at the NEF.

Editor's Note: Whether the NEF requests token for AF is FFS. The role of NEF in VFL is FFS.

Step 5. The NRF sends the access token to the NEF.

Step 6. The NEF sends the VFL service request (e.g., VFL preparation, sample alignment, feature alignment, VFL training, VFL inference) towards the FL clients, with the obtained token.

Step 7, 8a, 8b. The NWDAF containing MTLF acting as FL client verifies the received access token as specified in TS 33.501[5] clause 13.4.1. The NWDAF containing MTLF acting as FL client may also check the AF specific information (e.g., AF ID, AF provider/Vendor ID, Application ID, AF service ID) in the token for fine-grained authorization. In case of successful access token verification, the NWDAF containing MTLF acting as FL client sends a success VFL service response to the External AF acting as FL server, via the NEF.

Step 9. The Vertical Federated Learning procedure is performed between FL server (External AF) and FL client (NWDAF) via the NEF.

### 6.Y.3 Evaluation

Editor’s Note: Each solution should motivate how the potential security requirements of the key issues being addressed are fulfilled.

**\*\*\*\*** END of 2nd CHANGE **\*\*\*\***