**3GPP TSG-SA3 Meeting #116 *draft\_r1\_S3-242594***

Jeju, South Korea, 20th - 24th May 2024 *Revision of S3-242140*

**Source: Ericsson**

**Title: New Solution to KI#3:** **Privacy of VFL between VFL members**

**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 Rationale

This contribution proposes a solution to KI#3 "Privacy of VFL between VFL members". This solution proposes that in order to protect the UE ID privacy, e.g., during VFL sampling procedure, NEF needs to perform the UE ID mapping from internal UE IDs (SUPI) to External UE IDs (AF specific GPSI) and vice versa, and then forwards VFL service request.

# 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

[y] TS 23.501 V18.5.0 System architecture for the 5G System (5GS)

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

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

## 6.Y Solution #Y: Protection of Privacy of VFL between VFL members

### 6.Y.1 Introduction

This solution addresses Key Issue #3 “Privacy of VFL between VFL members". As stated in the key issue description,"The sample alignment procedure may involve the exchange of information (e.g. UE ID) which is sensitive and could potentially comprise the privacy of UEs."

This solution proposes that in order to protect the UE ID privacy, e.g. during VFL sampling procedure, NEF needs to perform the UE ID mapping from internal UE IDs (SUPI) to External UE IDs (AF specific UE Identifier) and vice versa, and then forwards VFL service request. According to TS 23.501[y] clause 5.20, "The AF specific UE Identifier shall not correspond to a MSISDN; it is represented as a GPSI in the form of an External Identifier. When used as an AF specific UE identifier, the External Identifier provided by the 5GCN shall be different for different AF". So, the privacy of UE ID is protected.

### 6.Y.2 Solution details

## In order to protect the UE ID privacy, NEF performs the UE ID mapping from internal UE IDs (SUPI) to External UE IDs (AF specific UE Identifier) and vice versa, and then forwards VFL service request/response.VFL service request can be a service related to Sample alignment, feature spaces alignment or jointly participating to train an ML model.

#### 6.Y.2.1 NWDAF acting as FL server



Figure 6.Y.2.1-1: Protection of Privacy of VFL between VFL members for NWDAF acting as FL server

Step 1. The NWDAF containing MTLF acting as VFL server sends the VFL service request/response to the NEF with Internal UE IDs, the Analytics ID information and the AF specific information.

Step 2. If internal UE IDs (SUPI) are received in step 1, the NEF performs internal UE IDs mapping to external UE IDs i.e., AF specific GPSI before forwarding the VFL service request/response.

Step 3a,3b. The NEF sends VFL service request/response to the AFs.NWDAF and AFs will do the VFL preparation phase, sample and feature alignment.

Step 4. The Vertical Federated Learning procedure is performed between FL server (NWDAF) and FL client (AF) via the NEF.

#### 6.Y.2.2 External AF acting as FL server



Figure 6.Y.2.2-1: Protection of Privacy of VFL between VFL members for External AF acting as FL server

Step 1. The External AF acting as VFL server sends the VFL service request/response to the NEF with AF specific external UE IDs, the Analytics ID information and the NWDAF specific information.

Step 2. If AF specific external UE IDs are received in step 1, the NEF performs AF specific external UE IDs mapping to internal UE IDs i.e., SUPI before forwarding the VFL service request/response.

Step 3a,3b. The NEF sends VFL service request/response to the NWDAFs.NWDAF and AFs will do the VFL preparation phase, sample and feature alignment.

Step 4. The Vertical Federated Learning procedure is performed between FL server (NWDAF) and FL client (AF) 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 **\*\*\*\***