|  |
| --- |
| 3GPP TR 33.784 V0.2.0 (2024-05) |
| Technical Report |
| 3rd Generation Partnership Project;Technical Specification Group Services and System Aspects;Study on security aspects of Core Network Enhanced Support for AIML (Release 19) |
|   |
|  |  |
| The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP.The present document has not been subject to any approval process by the 3GPPOrganizational Partners and shall not be implemented.This Specification is provided for future development work within 3GPPonly. The Organizational Partners accept no liability for any use of this Specification.Specifications and Reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices. |

|  |
| --- |
|  |
| ***3GPP***Postal address3GPP support office address650 Route des Lucioles - Sophia AntipolisValbonne - FRANCETel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16Internethttp://www.3gpp.org |
| ***Copyright Notification***No part may be reproduced except as authorized by written permission.The copyright and the foregoing restriction extend to reproduction in all media.© 2024, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).All rights reserved.UMTS™ is a Trade Mark of ETSI registered for the benefit of its members3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersLTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersGSM® and the GSM logo are registered and owned by the GSM Association |

Contents

Foreword 5

1 Scope 7

2 References 7

3 Definitions of terms, symbols and abbreviations 7

3.1 Terms 7

3.2 Symbols 8

3.3 Abbreviations 8

4 Overview 8

5 Key issues 8

5.1 Key Issue #1: Security aspects on enhancements to LCS to support AIML 8

5.1.1 Key issue details 8

5.1.2 Security Threats 8

5.1.3 Potential security requirements 9

5.2 Key Issue #2: Authorization mechanism of selection of VFL participants in the VFL group 9

5.2.1 Key issue details 9

5.2.2 Security threats 9

5.2.3 Potential security requirements 9

5.3 Key Issue #3: Privacy of VFL between VFL members 10

5.3.1 Description 10

5.3.2 Security threats 10

5.3.3 Potential security requirements 10

5.4 Key issue #4: Security of communication data used in VFL training process 10

5.4.1 Key issue details 10

5.4.2 Security threats 10

5.4.3 Potential security requirements 10

5.X Key Issue #X: <Key Issue Name> 11

5.X.1 Key issue details 11

5.X.2 Threats 11

5.X.3 Potential security requirements 11

6 Solutions 11

6.1 Solution #1: Security aspects on enhancements to LCS to support AIML 11

6.1.1 Introduction 11

6.1.2 Solution details 12

6.Y.3 Evaluation 13

6.2 Solution #2: LMF authorization mechanism in the AI/ML model retrieving scenarios 13

6.2.1 Introduction 13

6.2.2 Solution details 13

6.2.3 Evaluation 13

6.3 Solution #3: Solution for VFL member authorization 13

6.3.1 Introduction 13

6.3.2 Solution details 14

6.3.3 Evaluation 14

6.4 Solution #4: Authorization of VFL member selection 14

6.4.1 Introduction 14

6.4.2 Solution details 15

6.4.2.1 NWDAF is VFL Server 15

6.4.2.2 AF is VFL Server 16

6.4.3 Evaluation 17

6.5 Solution #5: Authorization of VFL participants involving NWDAF and AF for External AF acting as FL server 17

6.5.1 Introduction 17

6.5.2 Solution details 18

6.5.3 Evaluation 19

6.6 Solution #6: Authorization mechanism through NRF and NEF for AF outside the PLMN 19

6.6.1 Introduction 19

6.6.2 Solution details 20

6.6.3 Evaluation 21

6.7 Solution #7: Authorization for selection of participant NWDAF instances for the 3rd party AF-initiated federated learning 21

6.7.1 Introduction 21

6.7.2 Solution details 22

6.7.3 Evaluation 24

6.8 Solution #8: Authorization for selection of participant AF for the NWDAF-initiated federated Learning 24

6.8.1 Introduction 24

6.8.2 Solution details 25

6.8.3 Evaluation 26

6.9 Solution #9: UE ID privacy protection of VFL between VFL members 26

6.9.1 Introduction 26

6.9.2 Solution details 27

6.9.3 Evaluation 28

6.10 Solution #10: Privacy of data and sample alignment 28

6.10.1 Introduction 28

6.10.2 Solution details 28

6.10.3 Evaluation 29

6.11 Solution #11: Protection of Privacy of VFL between VFL members 29

6.11.1 Introduction 29

6.11.2 Solution details 29

6.11.2.1 NWDAF acting as FL server 30

6.11.2.2 External AF acting as FL server 31

6.11.3 Evaluation 31

6.12 Solution #12: VFL sample alignment initialled by NWDAF 31

6.12.1 Introduction 31

6.12.2 Solution details 31

6.12.3 Evaluation 33

6.13 Solution #13: Privacy protect mechanism for sample alignment 33

6.13.1 Introduction 33

6.13.2 Solution details 33

6.13.3 Evaluation 33

6.Y Solution #Y: <Solution Name> 33

6.Y.1 Introduction 33

6.Y.2 Solution details 33

6.Y.3 Evaluation 33

7 Conclusions 33

Annex <X> (informative): Change history 34

# Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

In the present document, modal verbs have the following meanings:

**shall** indicates a mandatory requirement to do something

**shall not** indicates an interdiction (prohibition) to do something

The constructions "shall" and "shall not" are confined to the context of normative provisions, and do not appear in Technical Reports.

The constructions "must" and "must not" are not used as substitutes for "shall" and "shall not". Their use is avoided insofar as possible, and they are not used in a normative context except in a direct citation from an external, referenced, non-3GPP document, or so as to maintain continuity of style when extending or modifying the provisions of such a referenced document.

**should** indicates a recommendation to do something

**should not** indicates a recommendation not to do something

**may** indicates permission to do something

**need not** indicates permission not to do something

The construction "may not" is ambiguous and is not used in normative elements. The unambiguous constructions "might not" or "shall not" are used instead, depending upon the meaning intended.

**can** indicates that something is possible

**cannot** indicates that something is impossible

The constructions "can" and "cannot" are not substitutes for "may" and "need not".

**will** indicates that something is certain or expected to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

**will not** indicates that something is certain or expected not to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

**might** indicates a likelihood that something will happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

**might not** indicates a likelihood that something will not happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

In addition:

**is** (or any other verb in the indicative mood) indicates a statement of fact

**is not** (or any other negative verb in the indicative mood) indicates a statement of fact

The constructions "is" and "is not" do not indicate requirements.

# 1 Scope

The present document studies the security aspects of enablers for network automation for the 5G system based on the outcome of TR 38.843[2] and TR 23.700-84[3]. More specifically, this document will identify security issues and requirements and provide corresponding security solutions related to the following scenarios:

- Study security aspects on enhancements to LCS to support AI/ML based Positioning considering the conclusions in TR38.843[2] and TR 23.700-84[3].

- Security aspects of cross-domain (i.e. 5G Core and AF) Vertical Federated Learning, including authorization of members of the VFL group and security aspects of enhancements on SA2 architecture to support VFL.

Editor’s Note: Based on the outcome of TR 38.843[2] and TR 23.700-84[3], security issues derived from WT#1.1, WT#1.2, and WT#1.3 of SP-231800 may be added to the scope of this study.

# 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

[7] 3GPP TS 23.288: “Architecture enhancements for 5G System (5GS) to support network data analytics services”.

[8] 3GPP TS 29.510: “Network Function Repository Services”.

[9] 3GPP TS 23.501: “System architecture for the 5G System (5GS)”.

# 3 Definitions of terms, symbols and abbreviations

## 3.1 Terms

For the purposes of the present document, the terms given in 3GPP TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [1].

**example:** text used to clarify abstract rules by applying them literally.

## 3.2 Symbols

For the purposes of the present document, the following symbols apply:

<symbol> <Explanation>

## 3.3 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

<ABBREVIATION> <Expansion>

# 4 Overview

Editor’s Note: This clause includes the overview applicable for the study.

TR 23.700-84 [3] defines core network enhanced support for Artificial Intelligence (AI)/Machine Learning (ML), all the architecture assumptions defined in this TR are also applicable to this study, and any security impact will be documented in the present document.

# 5 Key issues

Editor’s Note: This clause contains all the key issues identified during the study.

## 5.1 Key Issue #1: Security aspects on enhancements to LCS to support AIML

### 5.1.1 Key issue details

Based on conclusions in 3GPP TR 38.843 [2] and RAN approved WID RP-234039 [4], 5 use cases (i.e. case 1, 2a, 2b, 3a, 3b) which will be studied by RAN. And as agreed in TR 23.700-84 [3], only case 2b and case 3b (i.e. model is on the LMF) will be studied at this stage, and the main issue is to study model transition between LMF and NWDAF. For key issue about enhancements to LCS to support Direct AI/ML based Positioning in TR 23.700-84 [3], the following aspect will be investigated.

 Which entity trains the model for direct AI/ML positioning and if the entity that train the model and the consumer are different, how the model consumer gets the trained AI/ML model.

If AI model training entity and AI model consumer are different, since ML model is sensitive and it is belong to vendors, the authorization of ML model retrieval between LMF and NWDAF need to be considered.

### 5.1.2 Security Threats

In case of AI model training entity and AI model consumer are different:

- If there is no authentication and authorization mechanism for AIML model retrieval between model consumer and model training entity, AIML model may be leaked to unauthorized entities.

### 5.1.3 Potential security requirements

If AI model training entity and AI model consumer are different, 5GS shall support authentication and authorization of AIML model retrieval between LMF and NWDAF.

NOTE : The procedures defined in TS 33.501 [5] Annex X.10 Security for AI/ML model storage and sharing needs to be taken into account.

## 5.2 Key Issue #2: Authorization mechanism of selection of VFL participants in the VFL group

### 5.2.1 Key issue details

The TR 23.700-84 [3] studies the architecture enhancement to support VFL which allows the cooperation of NWDAFs containing MTLF and AFs to train an ML model in 3GPP networks.

In Rel-18, security of ML model sharing between NWDAFs has been studied as a part of Horizontal Federated Learning. However, vertical federated learning(VFL) between NWDAF and AF has not been studied (e.g. when the NWDAFs and/or AFs are in different domains, locations, regions etc). Hence, the authorizations of VFL client and VFL server to participate in the VFL process shall consider the scenario that the VFL participants (i.e., VFL client and VFL server) may be the NWDAF and AF.

After successful authorization among AF(s) and NWDAF(s) in the same VFL group, the AF(s) and NWDAF(s) may share information among the members for VFL.

This key issue studies the authorization aspects of VFL server and VFL clients in the VFL group Considering AF/NWDAF can operate as a VFL client/VFL Server. VFL members also called VFL participants and VFL participant can be active, or passive as defined in TR 23.700-84 [3].

### 5.2.2 Security threats

There are following threats that could occur during the VFL process:

If a VFL client joins a VFL group without being authorized by the VFL server, it may lead to the following issues:

- The unauthorized VFL client may affect the generation of VFL group's ML model negatively.

After authorization, if NWDAF shares network internal information to the external AFs, the operator’s internal information may be exposed.

### 5.2.3 Potential security requirements

5GS shall support the authorization of members involved in vertical federated learning (VFL) group including NWDAFs and/or AFs.

5GS shall support means to avoid internal information exposed to external VFL members.

Editor’s Note: Whether the VFL group needs to be authorized is FFS which is dependent on SA2’s progress.

Editor’s Note: The terms can be updated based on SA2’s progress.

Editor’s Note: The details of network internal information, e.g. NWDAF’s NF instance ID, is ffs. Whether network internal information will be shared with external AFs is ffs and will depend on SA2’s progress. Whether details of the internal network information are considered sensitive is FFS.

## 5.3 Key Issue #3: Privacy of VFL between VFL members

### 5.3.1 Description

Vertical federated learning (VFL) allows the cooperation of multiple NWDAF(s) and/or AF(s) to cooperate to train models locally where no raw data need to be exchanged.

As description in IEEE Guide for FL [6], Sample alignment module, a sample alignment module is mainly used for vertical federated machine learning. The module identifies the overlapped samples of different data sources and does not disclose sample feature information.

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.

### 5.3.2 Security threats

The UE ID privacy may be leaked between VFL participants from different domains when doing VFL, the AF may obtain UE information (UE ID) supported by another AF.

### 5.3.3 Potential security requirements

5GS shall support privacy protection on sample alignment procedure.

Editor’s Note: The terms can be updated based on SA2’s progress.

## 5.4 Key issue #4: Security of communication data used in VFL training process

### 5.4.1 Key issue details

Vertical federated learning (VFL) allows the cooperation of multiple NWDAF(s) and/or AF(s) to cooperate to train models locally where no raw data need to be exchanged.

After the selection of VFL clients and the completion of data and feature alignment procedures, the VFL training will commence between the VFL clients and VFL server. During this process, the VFL clients and VFL server will exchange intermediate results such as activations and gradients. Following the training, distinct local models will be present on both the VFL server and VFL clients, with the global model on the VFL server serving as the final output of the training process.

### 5.4.2 Security threats

Editor’s Note: The details of security threat need to be added.

### 5.4.3 Potential security requirements

TBA.

## 5.X Key Issue #X: <Key Issue Name>

### 5.X.1 Key issue details

### 5.X.2 Threats

### 5.X.3 Potential security requirements

# 6 Solutions

Table 6.0-1: Mapping of solutions to key issues

|  |  |
| --- | --- |
|  | **Key Issues** |
| **Solutions** | 1 | 2 | 3 | 4 |
| 1 | X |  |  |  |
| 2 | X |  |  |  |
| 3 |  | X |  |  |
| 4 |  | X |  |  |
| 5 |  | X |  |  |
| 6 |  | X |  |  |
| 7 |  | X |  |  |
| 8 |  | X |  |  |
| 9 |  |  | X |  |
| 10 |  |  | X |  |
| 11 |  |  | X |  |
| 12 |  |  | X |  |
| 13 |  |  | X |  |
|  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

## 6.1 Solution #1: Security aspects on enhancements to LCS to support AIML

### 6.1.1 Introduction

This solution is proposed to address Key Issue#1: Security aspects on enhancements to LCS to support AIML.

The AI/ML model retrieval and transition between the model training entity such as NWDAF and model consumer such as LMF is well investigated in TR 23.700-84 [3]. However, the AI/ML model training entity and AI/ML model consumer may be different; thereby the AIML model may be altered by the malicious entities and leaked to unauthorized entities. Therefore, the authorization of a trusted AI model consumer should be considered to communicate and performing a collaborative training process with AI/ML Model training entity.

The principle of this solution is to reuse model authorization procedure as much as possible description in clause X.10 in TS 33.501 [5]. If the AI model training entity and AI model consumer are different, AI model consumer shall be authorized to retrieval model from ML model training entity.

The LMF model may have its own service area which means it is allowed to obtain the UE location in this Area. However, if the LMF can get UE location using AIML model, the LMF could get the AIML model for LCS which service area is out of its LMF service area, the LMF may get UE location out of its service area.



**Figure 6.1.1-1**

As the result, 5GC shall authorize the LMF to get the Model which service area is within its service area so that the LMF cannot predict UE location out of its service area.

### 6.1.2 Solution details



**Figure 6.1.2-1 Authorization of AIML model procedure for LMF**

0a. NF Service producer i.e., NWDAF containing MTLF registers its NF profile in the NRF with Service Area and ML Model Interoperability indicator per Analytics ID as described in clause 5.2 of TS 23.288 [7].

0b. LMF registers its NF profile in the NRF with Vendor ID and service area.

0c. LMF discover the NWDAF containing MTLF using NRF discovery procedure.

1. The LMF sends an access token request to NRF as specified in clause 13.4.1. The access token request may contain the Analytics ID, Vendor ID and Area of Interest.

2. The NRF authorizes the LMF based upon the information received in step0b. The NRF shall check whether the Vendor ID of the LMF is within the Interoperability indicator for the Analytics ID. The NRF shall also verify the Area of Interest is within the Server Area of the LMF. 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 and Area of Interest.

3. The NRF sends the access token to the LMF, or rejects the request in case of failed authorization, as described in clause 13.4.1.4.

4. The LMF performs Nnwdaf\_MLModelProvision (Analytics ID, Vendor ID, Area of Interest and token) service operation at the NWDAF containing MTLF to retrieve ML models for the LCS.

6. The NWDAF containing MTLF verifies the received access token as specified in clause 13.4.1. The NWDAF containing MTLF check whether the Area of Interest is in the Area of Interest in the access token. In case of successful access token verification, the NWDAF containing MTLF sends a success response to the LMF.

Editor’s Note: Whether service area is needed is FFS.

### 6.1.3 Evaluation

TBD

## 6.2 Solution #2: LMF authorization mechanism in the AI/ML model retrieving scenarios

### 6.2.1 Introduction

The solution solves KI#1 (i.e., authorize LMF to retrieve AI/ML model from the NWDAF) by reusing mechanism defined in Annex X.10 of TS 33.501 [5].

### 6.2.2 Solution details

The existing authorization mechanism defined in Annex X.10 of TS 33.501 [5] is reused to authorize LMF with the following adaptations:

1. In step 0a, the ML Model Interoperability indicator is a list of LMF providers (vendors) that are allowed to retrieve ML models from the NWDAF containing MTLF.
2. In step 0b, NF Service consumer e.g., LMF registers at the NRF including its Vendor ID.

Editor's Note: Whether model storage at ADRF is relevant for models to be consumed at the LMF needs to be clarified

### 6.2.3 Evaluation

TBA

## 6.3 Solution #3: Solution for VFL member authorization

### 6.3.1 Introduction

This solution addresses KI#2.

The concept of the solution is similar to ‘X.9 Authorization of selection of participant NWDAF instances in the Federated Learning group’ defined in clause X.9 of TS 33.501 [5].

In the VFL case, NWDAF and/or AF can participate in the VFL process. Please note that internal AF information is available at the NRF as a part of AF's NFprofile and external AF information is also available at the NRF as a part of NEF NFprofile. Please refer to the section 6.1.6.2.48 NefInfo of TS 29.510 [8] that contains pdfData that contains AF connected via NEF.

### 6.3.2 Solution details

NWDAF/Internal AF or NEF (on behalf of external AF) updates their NFprofile in the NRF with VFL information, including its VFL capabilities (e.g. privacy protection supported/not supported, supported role (Client/Server/Active/Passive, etc.)), interoperability indicator per analytics. The NFprofile also includes allowed VFL capability per consumer.

The consumer NWDAF/AF or NEF (on behalf of external AF) sends an access token request to the NRF. The access token request may contain the Analytics ID, source NF, interoperability indicator/vendor Id and target NF's VLF capability for the requested VFL process.

The NRF authorises the NWDAF/Internal AF or NEF & external AF based upon the information received in step 1. If the authorization succeeds, NRF generates the access token with the claim, including the target VFL capability.

The consumer NWDAF/Internal AF or NEF (on behalf of external AF) sends the service request, including an access token, to the producer NWDAF/Internal AF or NEF. The producer verifies the token and allows the VFL procedure.

Editor’s Note: Capability and privacy protection details are FFS. Why VFL capability is per consumer is FFS.

Editor’s Note: Whether the NRF authorizes the NEF or external AF behind the NEF is ffs. Secondly when NEF registers AF details are FFS.

Editor’s Note: Rational for adding target VFL capability into token and how to verify it is ffs.

### 6.3.3 Evaluation

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

TBD

## 6.4 Solution #4: Authorization of VFL member selection

### 6.4.1 Introduction

The solution addresses the key issue #2 “Authorization mechanism of selection of VFL participants in the VFL group”.

The solution proposes to address two scenarios, i.e. NWDAF is VFL server, and AF is VFL server.

The solution also proposes to address NWDAF’s NF instance ID exposure issue.

The solution proposes the similar authorization mechanism of selection of HFL participants, i.e. use vendor ID and interoperability indicator. The difference is that considering NEF is intermediate node in VFL, the NEF will do authorization for secure communication and translation of internal-external information as depicted in clause 6.2.5.0 of TS 23.501 [9].

### 6.4.2 Solution details

#### 6.4.2.1 NWDAF is VFL Server



**Figure 6.4.2.1-1 Procedure of authorization of VFL member selection (NWDAF is VFL server)**

Editor’s Note: Motivation for NRF to authorize NWDAF on behalf of external AFs is ffs.

1. After the registration of AF (VFL Client) available data at NEF, the NEF invokes Nnrf\_NFManagement\_NFUpdate\_request service operation to update its registration information (i.e. NEF Profile) including the associated AF ID, the supported analytics ID(s), and the interoperability indicator of the AFs into the NEF profile.
2. NRF stores the received NEF registration information, and sends Nnrf\_NFManagement\_NFUpdate\_response message to the NEF.
3. When NWDAF (VFL Server) needs to discovery the available AFs and the appropriated NEF for VFL training, the NWDAF invokes Nnrf\_NFDiscovery\_Request\_request service operation.
4. The NRF matches the requested query for AFs with the registered NEF Profiles. It is assumed that AF ID1 and AF ID2 are selected.
5. The NRF sends Nnrf\_NFDiscovery\_Request\_response message to the NWDAF. The message includes the selected AF ID1 and AF ID2 and the associated NEF ID.

Editor’ Note: Whether AF has two AF IDs is FFS.

1. The NWDAF sends token request message to the NRF, the message includes the NF consumer ID (i.e. NWDAF ID), NF provider ID (i.e. NEF ID), VFL Client ID (i.e. AF ID1, AF ID2), requested analytics ID and vendor ID of the NWDAF.
2. The NRF checks whether the NWDAF could access AF, which includes checking whether AF is associated with NEF, whether NWDAF’s vendor ID is included in AFs’ interoperability indicator, whether AFs’ interoperability indicators are mutually inclusive, and whether analytics is included in AFs’ supported analytics. After successfully checking, the NRF signs token to the NWDAF, the token shall additionally include AF IDs and analytics ID.
3. The NRF sends token to the NWDAF.
4. The NWDAF sends request for VFL (e.g. sample alignment request) to the NEF. The request includes NWDAF ID, AF IDs, analytics ID and the token.
5. The NEF checks the token, including check integrity of the token, and check whether AF IDs are included in the token, and whether analytics ID is included in the token.
6. After successful checking, the NEF sends request for VFL to different AF.
7. The AF(s) sends response for VFL to the NEF.

#### 6.4.2.2 AF is VFL Server



**Figure 6.4.2.2-1 Procedure of authorization of VFL member selection (AF is VFL server)**

1. -2. NWDAF invokes Nnrf\_NFManagement\_NFRegister\_request service operation to register its registration information (i.e. NWDAF Profile) including the supported analytics ID(s), and the interoperability indicator of the NWDAFs.
2. When AF (VFL Server) needs to discovery the available NWDAFs for VFL training, the AF sends Discovery Request to NEF.
3. The NEF invokes Nnrf\_NFDiscovery\_Request\_request service operation.
4. The NRF matches the requested query for NWDAFs with the registered NWDAF Profiles. It is assumed that NWDAF ID1 and NWDAF ID2 are selected.
5. The NRF sends Nnrf\_NFDiscovery\_Request\_response message to the NEF. The message includes the selected NWDAF ID1 and NWDAF ID2.
6. The NEF anonymizes NWDAF IDs into multiple temporary NWDAF IDs, and stores the mapping. The NWDAF IDs is 1 to n mapping to the temporary NWDAF IDs so that the topology information will not be exposed, e.g. NWDAF numbers or NWDAF internal IDs are not exposed.

Editor’ Note: Whether there is a need to secure NF Instance ID of NWDAF and anonymization of NWDAF IDs is ffs.

1. The NEF sends Discovery Response message to the AF including the temporary NWDAF IDs.
2. The AF sends VFL request (e.g. sample alignment request) to the NEF. The request includes AF IDs, temporary NWDAF IDs, and analytics ID.
3. The NEF conveys the temporary NWDAF IDs into NWDAF IDs
4. The NEF sends token request message to the NRF, the message includes the NF consumer ID (i.e. NEF ID), NF provider ID (i.e. NWDAF ID), VFL Server ID (i.e. AF ID), requested analytics ID and vendor ID of the AF.
5. The NRF checks whether the AF could access NWDAFs, which includes checking whether AF is associated with NEF, whether AF’s vendor ID is included in NWDAFs’ interoperability indicator, whether NWDAFs’ interoperability indicators are mutually inclusive, and whether analytics is included in NWDAFs’ supported analytics. After successfully checking, the NRF signs token to the NEF, the token shall additionally include analytics ID.
6. The NRF sends token to the NWDAF.
7. The NEF sends VFL request (e.g. sample alignment request) to the NWDAFs. The request includes NWDAF ID, NEF ID, analytics ID and the token.
8. The NWDAF checks the token, including check integrity of the token, and check whether analytics ID is included in the token.
9. The NWDAF(s) sends response for VFL to the AF.

### 6.4.3 Evaluation

TBA.

## 6.5 Solution #5: Authorization of VFL participants involving NWDAF and AF for External AF acting as FL server

### 6.5.1 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.

### 6.5.2 Solution details

****

**Figure 6.5.2-1: 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[7]. 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.

### 6.5.3 Evaluation

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

## 6.6 Solution #6: Authorization mechanism through NRF and NEF for AF outside the PLMN

### 6.6.1 Introduction

This solution addresses KI#2: Authorization mechanism of selection of VFL participants in the VFL group

The TR 23.700-84 [3] studies the architecture enhancement to support VFL which allows the cooperation of multiple NWDAFs containing MTLF to train an ML model in 3GPP networks. The NWDAF may interact with an AF to collect data from UE applications as a data input for analytics generation. In case when AF is located outside the MNO, the NEF is used to exchange the messages between the AF the NWDAF. The authorizations of VFL client and VFL server to participate in the VFL process shall consider the scenario that the VFL participants (i.e., VFL client and VFL server) may be the NWDAF and AF.

This solution addresses the authorization aspects of VFL server in the VFL group through NRF and NEF.

### 6.6.2 Solution details

The Figure 6.6.2-1 describes the detailed authorization mechanism for of NWDAF acting as VFL server in the VFL group.

**Figure 6.6.2 -1: Authorization mechanism through NRF and NEF for AF outside the PLMN**

1. VFL Participants (e.g., VFL active Participant, VFL passive Participant, VFL server Participant) register the NF profiles with the NRF. The NF profiles include the VFL Participant, Analytics ID, Vendor ID or Application Name, and VFL Interoperability indicators. The VFL Interoperability ID is a list of Vendor IDs. If the AF is also in the VFL group, the VFL Interoperability ID also includes Application Name or AF Identifier(s). In addition, the optional parameter in NF profile includes one or more security parameters such as serving UE range.
2. The NWDAF requests an access token from the NRF. The NWDAF sends a service request for an AF to join the VFL group through NEF. The access token request sent to the NRF includes the NEF ID, AF ID and Analytics ID. In addition, optional parameter includes Vendor ID, VFL Interoperability ID and training UE range.
3. The NRF finds the NF profile registered by the NEF based on the NEF ID and obtains the information about the AF vertical federated authorization scope (the information updated by the NRF in step 1). The NRF shall verify the VFL Interoperability ID in the token request is within the VFL Interoperability ID(s). The NRF may also verify the training UE range is in the scope of Serving UE range. If the authorization succeeds, NRF generates the access token(s) as specified in clause 13.4.1. Optionally, the access token includes parameters such as an AF ID, VFL Interoperability ID and a training UE range.
4. The NRF sends the generated access token to the NWDAF. If the authorization check in step 3 fails, a rejection message is sent.
5. If the NWDAF obtains the access token, the NWDAF sends a service request message to the NEF for requesting an AF to join the VFL group. The message contains the AF ID, Analytics ID and access token.
6. If the verification is successful, the NEF obtains the Analytics ID contained in the access token and verifies whether it is the same as the Analytics ID received in step 5. If the access token contains optional parameters, the NEF obtains the Analytics ID contained in the access token.
* If the AF ID is included within the token, the system checks whether the AF ID is the same as the AF ID requested in step 5.
* If the message contains parameters such as training UE range, the NEF adds the parameters to the message in step 7 and sends the message to the AF to indicate some security capabilities in the VFL process.
1. The NEF sends a request to the AF for joining the VFL group. The request contains the Analytics ID and token.
2. The VFL client (e.g., AF) determines whether to join the network based on the local policy. The VFL client check whether the VFL Interoperability ID is matching with the VFL Interoperability ID in the access token.
3. In case of successful access token verification, the AF sends a success response to the VFL server through NEF. Otherwise, the AF sends a failure response.
4. If the NEF receives a success response, the NEF sends a success response to the NWDAF.

Editor’s Note: The optional security parameters, i.e. serving UE range and training UE range are FFS.

Editor’s Note: The validation of the access token at the AF and the clarification on token transmission to the AF is FFS.

### 6.6.3 Evaluation

TBD

## 6.7 Solution #7: Authorization for selection of participant NWDAF instances for the 3rd party AF-initiated federated learning

### 6.7.1 Introduction

The solution addresses part of KI#2 (i.e. Authorization of selection of participant NWDAF instances for AF-initiated Federated Learning)

In this solution, the 3rd party AF requests the NWDAF to participate in federated learning task via the NEF.

The NEF requests the NWDAF-related token on behalf of the AF.

The NRF uses NWDAF's NF profile to authorize the 3rd party AF to select a specific NWDAF NF instance as the federated learning client.

The token issued to the NEF contains the AF identifier, NF instance ID of NEF, and the NF instance ID of NWDAF.

The NWDAF authorizes the federated learning-related service from the AF via the token and certificate/CCA of the AF.

### 6.7.2 Solution details



**Figure 6.7.2-1 Authorization of federated learning related service request**

If AF has no knowledge about NWDAF identifiers (e.g., NF instance ID of NWDAF), step1 to step 6 and step 8 to step 14 are executed.

If AF has knowledge about NWDAF identifiers (e.g., NF instance ID of NWDAF), step7 to step 14 are executed.

0. The NWDAF registers to the NRF. After the registration, NF profile of NWDAF is stored in the NRF. NF profile indicates the capability of the NWDAF. The capability includes NWDAF can serve as the FL client, the NWDAF can serve as the FL server, the NWDAF can serve as FL server as well as FL client. The profile also includes Federated learning partner Indicator indicating the AF identifiers and/or NF instance identifier that can support the ML model type of NWDAF.

1. The AF sends the federated learning related service request to the NEF. The request includes the AF identifier (e.g., the FQDN), expected NF type (i.e. NWDAF), expected NWDAF capability (i.e. FL client). The request also contains the certificate or CCA (Client Credentials Assertion) of the AF.

Editor's Note: Why the need to use CCA for external AF to participate in the VFL group is FFS.

Editor's Note: The term and service name shall be aligned with SA2 specification.

1. The NEF authorizes the AF to trigger the service based on the local policy or OAuth 2.0.
2. If the AF is authorized to trigger the service, the NEF triggers Nnrf\_NFDiscovery\_Request to get NWDAF identifiers (e.g., NF instance ID, FQDN of NWDAF). The request includes the NF type (i.e. NWDAF), the NEF identifier (e.g., NF instance ID of NEF), expected federated learning related service name and the AF identifier (e.g., the FQDN). The request also contains the certificate or CCA (Client Credentials Assertion) of the AF.
3. The NRF validates the certificate or CCA of the AF for authenticating the AF. Then the NRF authorizes the request based on NWDAF NF profile which contains the AF(s) supporting ML model type of NWDAF, the FQDN of the AF and requested NWDAF capability.
4. If the AF is authorized to discover the requested NWDAF(s), the NRF sends the response to the NEF. The response includes the NWDAF identifier(s) (e.g., NF instance ID of NWDAF) that fulfill the requirement presented in step 1.
5. The NEF sends the received NWDAF identifier(s) to the AF.
6. The AF sends the federated learning related service request to the NEF. The request includes the AF identifier (e.g., the FQDN) and NWDAF identifier. The request also contains the certificate or CCA (Client Credentials Assertion) of the AF.
7. The NEF sends the token request to the NRF. The token request includes the expected federated learning related service, AF identifier (e.g., the FQDN) and NWDAF identifier (e.g., the NF instance ID, FQDN). The token request contains the certificate or CCA (Client Credentials Assertion) of the AF.
8. The NRF validates the certificate or CCA of the AF for authenticating the AF. Then the NRF authorizes the request based on the NWDAF's NF profile and local policy.
9. If the AF is authorized to request the service, the NRF sends the token to the NEF. The token includes the expected federated learning service name, AF identifier (e.g., the FQDN), NEF identifier (e.g., the NF instance ID of the NEF), and NWDAF identifier (e.g., the NF instance ID, FQDN).
10. The NEF sends the federated learning related service request to the target NWDAF. The request includes the AF identifier (e.g., the FQDN), the NEF identifier, the token, and certificate/CCA of the AF.
11. The NWDAF authenticates the AF by one of the methods described in 3GPP TS 33.501 [1] clause 13.3.2.2 and if successful, it verifies the token as described in 3GPP TS 33.501 [1] clause 13.4.1.1. The NWDAF shall verify the token as follows:

The NWDAF checks if the audience claim of the token matches its own identifier.

The NWDAF checks if the subject claim in the token matches the identifier of the NEF.

The NWDAF checks if the AF identifier in the token matches the subject claim of the CCA.

If scope or "additional scope" (i.e. the expected federated learning related service) is present, the NWDAF checks that the scope or "additional scope" matches the requested service operation.

The NWDAF checks that the token has not expired by verifying the expiration time in the token against the current data/time.

If all the checks are successful, the token is validated. If any of the checks fails, the authorization procedure should be terminated.

1. If the information in the request is allowed by successful validation of the token, the NWDAF sends federated learning related response (e.g., sample information including UE ID) to the NEF. Otherwise, the NWDAF rejects the request.
2. The NEF sends federated learning related response (e.g., sample information including UE ID) to the AF.

### 6.7.3 Evaluation

TBA

## 6.8 Solution #8: Authorization for selection of participant AF for the NWDAF-initiated federated Learning

### 6.8.1 Introduction

The solution addresses part of KI#2 (i.e. Authorization of selection of AF for NWDAF -initiated Federated Learning)

In this solution, the NWDAF requests the 3rd party AF to participate in federated learning task via the NEF.

The NRF uses NEF's NF profile to authorize the NWDAF to select a specific AF as the federated learning client.

The token issued to the NWDAF contains the AF identifier, NF instance ID of NEF, and the NF instance ID of NWDAF.

The NEF authorizes the federated learning-related service via the token of the NWDAF.

### 6.8.2 Solution details



**Figure 6.8.2-1 Authorization of sensing related service.**

Step 1 to step 3 are optional.

This solution does not address the NWDAF NF instance ID protection issue.

If NWDAF has obtained the AF identifier(s) via the previous procedures, then Step 1 to step 3 can be skipped.

1. AF registers its profile to the NRF via the NEF.
2. NWDAF triggers Nnrf\_NFDiscovery\_Request to get AF identifiers (e.g., FQDN of the AF). The request includes the expected NF type (i.e. NEF), the expected AF capability (i.e., AF can serve as the FL client or the AF can serve as FL server as well as FL client), the expected service name (i.e., the federated learning related service), the expected federated learning model type (e.g., the model type may be indicated by the analytic ID), and the NWDAF identifier (e.g., the NF instance ID of the NWDAF).

Editor's Note: The term and service name in this solution shall be aligned with SA2

Editor's Note: Motivation for NRF to authorize the NWDAF to access services of external AF is FFS

1. The NRF authorizes the request based on NF profile of NEF and local policy. The NF profile of NEF includes the AF identifier, the corresponding AF capability, the federated learning Model supported by the AF.
2. If the NWDAF is authorized, the NRF sends the discovered NEF identifier(s) (e.g., the NF instance ID of the NEF) and AF identifier(s) (e.g., the FQDN) to the NWDAF.
3. The NWDAF sends the token request to the NRF. The token request includes the NEF identifier (e.g., the NF instance ID of the NEF), the AF identifier(s) (e.g., the FQDN), the expected AF capability (i.e., AF can serve as the FL client or the AF can serve as FL server as well as FL client), the expected service name (i.e., the federated learning related service), the expected federated learning model type (e.g., the model type may be indicated by the analytic ID), and the NWDAF identifier (e.g., the NF instance ID of the NWDAF).
4. The NRF authorizes the request based on the NEF's NF profile and local policy. The NF profile of NEF includes the required information (e.g. AF capability, federated learning model types supported by the AF (e.g., the model type can be indicated by the analytic ID), AF identifier) in the profile of the AF.

If the NWDAF is authorized to request the service, the NRF sends the token to the NWDAF. The token includes the allowed service (i.e., the federated learning related service), NEF identifier (e.g., the NF instance ID, FQDN), AF identifier (e.g., the FQDN) and NWDAF identifier (e.g., the NF instance ID, FQDN). The audience claim of the token is NEF identifier (e.g., the NF instance ID). The subject claim of the token is NWDAF identifier (e.g., the NF instance ID). The expected service (i.e., the federated learning related service) and AF identifier (e.g., the FQDN) are included in the additional scope of the token.

1. NWDAF sends the federated learning related service request to the NEF. The federated learning related service request includes the AF identifier (e.g., the FQDN) and NWDAF identifier (e.g., the NF instance ID, FQDN) and the token.
2. The NEF verifies the token and check the service request against the verified token.

The NEF checks if the audience claim of the token matches its own identifier.

The NEF checks if the subject claim of the token matches the subject claim of the certificate of the NWDAF.

If scope or "additional scope" (i.e. allowed service and AF identifier) is present, the NEF checks that the scope or "additional scope" matches the federated learning related service request message.

The NEF checks that the token has not expired by verifying the expiration time in the token against the current data/time.

If all the checks are successful, the token is validated. If any of the checks fails, the authorization procedure should be terminated.

1. If the information in the request is allowed by the token, the NEF forwards the request to the AF.

Otherwise, the NEF rejects the request.

1. The AF sends the federated learning related service response (e.g., AI/ML model) to the NEF.
2. NEF sends the federated learning related service response (e.g., AI/ML model) to the NWDAF.

### 6.8.3 Evaluation

TBA

## 6.9 Solution #9: UE ID privacy protection of VFL between VFL members

### 6.9.1 Introduction

This solution is proposed to address Key Issue#3: Privacy of VFL between VFL members.

As description of KI#3, the UE ID privacy may be leaked between VFL participants from different domains when doing VFL, the AF may obtain UE information (UE ID) supported by another AF. In clause 6.4.4 of TS 23.288 [2], for Analytics ID for observed service experience, the consumer needs to request the Analytics ID "Service Experience" for a UE identified by a SUPI or a group of UEs identified by a list of Internal Group-Ids in the procedure. In this case, the UE ID (e.g., SUPI, GPSI, AF specific UE identifier) may need to be shared to the VFL participants (e.g., NWDAF(s), AF(s)). However, The AF specific UE identifier is ensured to be unique across different AFs as defined in TS 23.003 [3], which means the different AF have different UE IDs for the specific UE. For example, UE1 is the user for both AF1 and AF2. The AF1 specific UE ID of UE1 is different from the AF2 specific UE ID of UE1.

The sample alignment procedure may involve the exchange of information (e.g., UE ID) which is sensitive and could potentially compromise the privacy of UEs.

The basic principle for this solution is that VFL participants only know the overlapped samples IDs and don’t know any other information in the sample alignment procedure. This solution introduces a new network functionality for sample alignment which can be supported by the NEF or new NF (VFL Coordinator).

The main functionality for the VFL Coordinator is to assist the VFL active doing VFL sample alignment and assign new VFL sample ID(s) for the overlapped sample ID(s). It is helpful for VFL members to improve the efficiency of VFL when doing VFL, for example, avoid sample ID mapping in the VFL, especially for the NEF.

### 6.9.2 Solution details



**Figure 6.9.1-1 Sample alignment procedure**

0a-0c. The VFL entities (e.g., VFL active Participant, VFL passive Participant, VFL Coordinator) register its supported VFL Interoperability ID(s). The VFL Interoperability ID is a list of Vendor IDs. If the AF is also in the VFL group, the VFL Interoperability ID also includes Application Name or AF Identifier(s).

1. VFL Active Participant discoveries the VFL members via NRF by invoking the NF discovery.

2. VFL Active Participant sends sample alignment request to the VFL Coordinator including the VFL Interoperability ID and VFL members.

3. VFL Coordinator sends VFL sample information request to each VFL members received in the step2.

4. VFL members return the supported sample ID(s) to the VFL Coordinator. If the Sample ID(s) is external UE ID(GPSI), the NEF may map the external UE ID to the Internal UE ID(SUPI).

NOTE: How VFL Participants determine the returned sample ID(s) is up to SA2.

5. This step is same with step3.

6. This step is same with step4.

7. VFL Coordinator determines the intersection sample ID(s) of the VFL members and may assign VFL sample ID(s). The VFL sample ID is new sample ID for the intersection of sample ID(s) which is same among all VFL members.

8a. VFL Coordinator returns the intersection sample ID(s) and VFL sample ID(s) to the VFL Active Participant.

8b. VFL Coordinator returns the intersection sample ID(s) and VFL sample ID(s) to the VFL Passive Participant(s).

9. All VFL members determine the overlapped VFL sample ID(s).

Editor’s Note: VFL coordinator architecture alignment is depending on the progress of SA2 and is FFS.

Editor’s Note: Clarification on VFL Interoperability ID is FFS.

Editor’s Note: Clarification on sample ID if this is UE ID or identifier that represent set of UE ID’s is FFS.

Editor’s Note: Clarification on VFL sample ID is FFS.

### 6.9.3 Evaluation

TBD

## 6.10 Solution #10: Privacy of data and sample alignment

### 6.10.1 Introduction

The solution addresses the key issue #3 “Privacy of VFL between VFL members”.

The solution proposes to use NEF to do sample alignment so that the external AF will not know internal sample ID list.

### 6.10.2 Solution details



**Figure 6.10.2-1 Procedure of Privacy of data and sample alignment**

1. VFL Server has already completed VFL clients discovery.

NOTE: Authorization procedure of VFL clients discovery is not in scope of this solution.

1. VFL Sever sends Sample alignment request including its sample ID list 1 to NEF, the sample ID list contain UE ID list (e.g. SUPI, GPSI).
2. NEF sends Sample alignment request to the VFL clients in the same VFL group.
3. VFL Clients reply Sample alignment response to the NEF. The Sample alignment response includes sample ID list 2 and 3.
4. The NEF determines the common sample ID list 4 based on the common part of all the sample ID list from VFL Server and Clients. In case of AF as VFL server, the NEF may do ID conversion to translate GPSI to SUPI through UDM. In case of NWDAF as VFL server, the NEF may do ID conversion to translate SUPI to GPSI through UDM.
5. The NEF sends notify message to VFL server and clients including the common sample ID list 4.

### 6.10.3 Evaluation

The solution addresses the key issue #3.

The solution proposes to use NEF to do sample alignment so that the external AF will not know internal sample ID list.

Editor’s Note: What’s the role of NEF in VFL depends on SA2 progress and whether there is a need to have GPSI to SUPI conversion by NEF is FFS.

## 6.11 Solution #11: Protection of Privacy of VFL between VFL members

### 6.11.1 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 [11] 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.

### 6.11.2 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.

Editor's Note: Whether the conversion between internal UE ID to external UE ID is needed is FFS.

#### 6.11.2.1 NWDAF acting as FL server

****

**Figure 6.11.2.1-1: 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.

#### 6.11.2.2 External AF acting as FL server



**Figure 6.11.2.2-1: 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.

### 6.11.3 Evaluation

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

## 6.12 Solution #12: VFL sample alignment initialled by NWDAF

### 6.12.1 Introduction

This solution addresses the security requirement of KI #3: Privacy of VFL between VFL members, and it proposes a preparation process used to have a negotiation between VFL Active Participant (VFL server) (i.e. NWDAF) and VFL Passive Participant (VFL client) (i.e. AF) to ensure they share the same sample space, i.e. same UEs before the VFL model training.

### 6.12.2 Solution details

This solution describes the VFL sample alignment initialled by NWDAF, as shown in the following figure 6.12.2-1.



**Figure** **6.12.2-1: VFL sample alignment initialled by NWDAF**

1. The NWDAF as the active participant (or VFL server) triggers the VFL operation with one or more AFs as the passive participant (or VFL client). To ensure all the participants share the same sample space, the NWDAF sends the VFL sample and feature alignment request to the NEF, including the samples (i.e. internal UE IDs) and feature profiles the NWDAF wants to use for the VFL training.
2. The NEF maps the internal UE ID to external UE ID. The NEF may retrieve UE’s external ID from the UDM.
3. The NEF sends the VFL sample and feature alignment request to all the VFL passive participant AF.

For one or more VFL passive participant AFs:

1. The AF(s) may down-select UEs from the received external UE IDs to ensure the samples are same among NWDAF and AF(s). On the other side, the feature in the same samples should be different among NWDAF and AF(s).
2. The AF sends the VFL sample and feature alignment response to the NEF, including selected external UE ID and feature profiles.
3. If multiple AFs involved, the NEF collects the sample and feature alignment response from AFs, and maps the external UE IDs to the internal UE IDs. The NEF selects the intersection of UE IDs in these responses.
4. The NEF sends the VFL sample and feature alignment response to the NWDAF, including the internal UE ID and feature profiles.
5. The NEF sends the VFL sample and feature alignment notify to the AF(s), including the external ID and feature profiles.

Editor’s Note: Whether the UE external ID should be sent to the AF before the VFL sample alignment is FFS.

Editor’s Note: Security aspects of feature alignment is FFS and whether feature alignment is needed is FFS.

Editor’s Note: which entity performs the sample alignment should be aligned with SA2, which is FFS.

### 6.12.3 Evaluation

TBD.

## 6.13 Solution #13: Privacy protect mechanism for sample alignment

### 6.13.1 Introduction

The following privacy leakage threat is considered in the KI#3.

The privacy is that VFL member A may get the User information(overlapped) of VFL member B when doing VFL.  For example, two VFL members A and B. UEx is UE GPSI, A support do VFL using UE [1,2,3],  B support do VFL using UE [2,3,4].  The privacy is that A could know B doing VFL support UE4.  The fact is that A and B shall only know UE[2,3] after sample alignment. The overlapped sample information is UE2,3,  and  UE1 and UE4 is not included. If the A know UE4 is the user of B or B know UE1 is the user of A, then the privacy is leak.

The solution addresses KI#3 (i.e., privacy protection on sample alignment procedure) by using NWDAF to do the sample alignment.

### 6.13.2 Solution details

If NWDAF is the VFL server and does the sample alignment, one AF cannot know the extra UE information of another AF except the overlapped UE information.

Editor's Note: How to enable privacy protection for AF initiated federated learning is FFS.

Editor's Note: The procedure shall be aligned with SA2.

### 6.13.3 Evaluation

TBA

## 6.Y Solution #Y: <Solution Name>

### 6.Y.1 Introduction

Editor’s Note: Each solution should list the key issues being addressed.

### 6.Y.2 Solution details

### 6.Y.3 Evaluation

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

# 7 Conclusions

Editor’s Note: This clause contains the agreed conclusions that will form the basis for any normative work.

Annex <X> (informative):
Change history

|  |
| --- |
| **Change history** |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2024-04 | SA3#115Adhoc-e | S3-241287 |  |  |  | TR skeleton for TR 33.784 | 0.0.0 |
| 2024-04 | SA3#115Adhoc-e | S3-241651 |  |  |  | S3-241290, S3-241621, S3-241639, S3-241615, S3-241624 | 0.1.0 |
| 2024-05 | SA3#116 | S3-242609 |  |  |  | S3-242584, S3-242585, S3-242586, S3-242587, S3-242588, S3-242589, S3-242590, S3-242591, S3-242592, S3-242593, S3-242594, S3-242595, S3-242596, S3-242597, S3-242669 | 0.2.0 |