|  |  |
| --- | --- |
| 3GPP TR 33.784 V0.5.0 (2024-11) | |
| 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 address  3GPP support office address  650 Route des Lucioles - Sophia Antipolis  Valbonne - FRANCE  Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16  Internet  http://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 members  3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners LTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners  GSM® and the GSM logo are registered and owned by the GSM Association |

Contents

Foreword 6

1 Scope 8

2 References 8

3 Definitions of terms, symbols and abbreviations 9

3.1 Terms 9

3.2 Symbols 9

3.3 Abbreviations 9

4 Overview 9

5 Key issues 9

5.1 Key Issue #1: Security aspects on enhancements to LCS to support AIML 9

5.1.1 Key issue details 9

5.1.2 Security Threats 10

5.1.3 Potential security requirements 10

5.2 Key Issue #2: Authorization mechanism of candidate VFL participants for the same VFL process 10

5.2.1 Key issue details 10

5.2.2 Security threats 10

5.2.3 Potential security requirements 11

5.3 Key Issue #3: Privacy of VFL between VFL participants 11

5.3.1 Description 11

5.3.2 Security threats 11

5.3.3 Potential security requirements 11

5.4 Key issue #4: Security of communication data used in VFL training process 11

5.4.1 Key issue details 11

5.4.2 Security threats 11

5.4.3 Potential security requirements 12

5.X Key Issue #X: <Key Issue Name> 12

5.X.1 Key issue details 12

5.X.2 Threats 12

5.X.3 Potential security requirements 12

6 Solutions 12

6.1 Solution #1: Security aspects on enhancements to LCS to support AIML 12

6.1.1 Introduction 12

6.1.2 Solution details 13

6.1.3 Evaluation 14

6.2 Solution #2: LMF authorization mechanism in the AI/ML model retrieving scenarios 14

6.2.1 Introduction 14

6.2.2 Solution details 14

6.2.3 Evaluation 14

6.3 Solution #3: Solution for VFL member authorization 15

6.3.1 Introduction 15

6.3.2 Solution details 15

6.3.2.1 AF (VFL Server) requesting the NWDAF 15

6.3.2.1 NWDAF (VFL Server) requesting the AF 16

6.3.3 Evaluation 17

6.4 Solution #4: Authorization of VFL member selection 17

6.4.1 Introduction 17

6.4.2 Solution details 18

6.4.2.1 NWDAF is VFL Server 18

6.4.2.2 AF is VFL Server 19

6.4.3 Evaluation 20

6.5 Solution #5: Authorization of VFL participants involving NWDAF and AF 21

6.5.1 Introduction 21

6.5.2 Solution details 22

6.5.2.1 External AF acts as VFL Server 22

6.5.2.2 NWDAF acts as VFL Server and external AF as VFL client 24

6.5.3 Evaluation 25

6.6 Solution #6: Authorization mechanism through NRF and NEF for AF outside the PLMN 25

6.6.1 Introduction 25

6.6.2 Solution details 25

6.6.3 Evaluation 27

6.7 Solution #7: Authorization for selection of participant NWDAF instances for the 3rd party AF-initiated federated learning 27

6.7.1 Introduction 27

6.7.2 Solution details 28

6.7.3 Evaluation 30

6.8 Solution #8: Authorization for selection of participant AF for the NWDAF-initiated federated Learning 30

6.8.1 Introduction 30

6.8.2 Solution details 31

6.8.3 Evaluation 32

6.9 Solution #9: UE ID privacy protection of VFL between VFL members 33

6.9.1 Introduction 33

6.9.2 Solution details 33

6.9.3 Evaluation 35

6.10 Solution #10: Privacy of sample alignment 35

6.10.1 Introduction 35

6.10.2 Solution details 35

6.10.3 Evaluation 36

6.11 Solution #11: Protection of Privacy of VFL between VFL members 36

6.11.1 Introduction 36

6.11.2 Solution details 36

6.11.2.1 NWDAF acting as FL server 37

6.11.2.2 External AF acting as FL server 37

6.11.3 Evaluation 38

6.12 Solution #12: VFL sample alignment initialled by NWDAF 38

6.12.1 Introduction 38

6.12.2 Solution details 39

6.12.3 Evaluation 40

6.13 Solution #13: Privacy protect mechanism for sample alignment 40

6.13.1 Introduction 40

6.13.2 Solution details 40

6.13.3 Evaluation 40

6.14 Solution #14: Authorization for LCS Data Storage and Retrieval 40

6.14.1 Introduction 40

6.14.2 Solution details 41

6.14.3 Evaluation 42

6.15. Solution #15: Reuse the existing SBA mechanisms for protection of communication data in VFL training process. 42

6.15.1 Introduction 42

6.15.2 Solution details 43

6.15.3 Evaluation 43

6.16 Solution #16: LMF authorization for AI/ML model retrieval from NWDAF containing MTLF 43

6.16.1 Introduction 43

6.16.2 Solution details 43

6.16.3 Evaluation 45

6.17 Solution #17: Privacy of VFL between VFL members 45

6.17.1 Introduction 45

6.17.2 Solution details 45

6.17.2.1 General procedures 45

6.17.3 Evaluation 46

6.Y Solution #Y: <Solution Name> 46

6.Y.1 Introduction 46

6.Y.2 Solution details 46

6.Y.3 Evaluation 46

7 Conclusions 47

7.1 Conclusion on Key Issue #1 47

7.2 Conclusion on Key issue #2 47

7.3 Conclusion on Key Issue #3 47

7.4 Conclusion on Key issue #4 47

Annex <X> (informative): Change history 48

# 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 identifies security issues and requirements and provides corresponding security solutions related to the following scenarios:

- Security aspects on enhancements to LCS to support AI/ML based Positioning considering the conclusions in TR 38.843[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 the architecture in TR 23.700-84 [3] to support VFL.

# 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] 3GPP TR 33.738: "Study on security aspects of enablers for Network Automation for 5G".

[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)".

[10] 3GPP TS 33.210: "Network Domain Security (NDS); IP network layer security"

# 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].

## 3.2 Symbols

Void

## 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].

AI Artificial Intelligence

LCS Location Service

ML Machine Learning

VFL Vertical Federated Learning

# 4 Overview

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

# 5 Key issues

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

### 5.1.1 Key issue details

Based on conclusions in TR 38.843 [2], and as described in TR 23.700-84 [3], only case 2b and case 3b (i.e. model is on the LMF) are 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 are 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.*

Besides, the AI/ML model training entity (e.g., an NWDAF containing an MTLF) can obtain training data for AI/ML-based positioning from data sources such as the LMF and/or ADRF.

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

The LMF collects input data for training an AI/ML Model for UE Positioning, or for invoking by NWDAF for AI/ML positioning model training or model performance monitoring. The input data includes location related information of UE(s), hence the LMF should choose those UE(s) with permission.

There can be a need to consider towards compliance to regional legislation for direct AI/ML based positioning and to obtain user consent for UE data collection.

### 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 or training data retrieval between model consumer and model training entity, AIML model or training data 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 or training data 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 need to be taken into account.

## 5.2 Key Issue #2: Authorization mechanism of candidate VFL participants for the same VFL process

### 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.

The security of ML model sharing between NWDAFs has been studied as a part of Horizontal Federated Learning in TR 33.738[4]. 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 same 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) for the same VFL process, the AF(s) and NWDAF(s) may share information among the participants for VFL.

This key issue studies the authorization aspects of VFL server and VFL clients in the same VFL process Considering AF/NWDAF can operate as a VFL client/VFL Server. The 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 is selected without being authorized by the VFL server, it may lead to the following issues:

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

If the external AF acting as a VFL server is unauthorized, it may lead to the following issues:

- The unauthorized VFL server 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 candidate VFL participants involved in the same vertical federated learning (VFL) process including NWDAFs and/or AFs.

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

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

### 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.

## 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 sample 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 loss information and gradients information. To secure the data in transit, these exchanges are encrypted to prevent interception and ensure data integrity. 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

Without integrity protection, the communication data used in VFL training process may be manipulated or forged by an attacker, potentially affecting the accuracy of the training model.

Without confidentiality protection, the communication data used in VFL training process may be exposed, enabling attackers to use the result to train their own models.

If the communication data exchanged between VFL participants is not anti-replay protected, the communication data may be replayed.

### 5.4.3 Potential security requirements

The 5GC shall support integrity, confidentiality and replay protection for communication data used in VFL training process.

NOTE: The existing SBA security can be reused where applicable.

# 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 |  |
| 14 | X |  |  |  |
| 15 |  |  |  | X |
| 16 | X |  |  |  |
| 17 |  |  | 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.

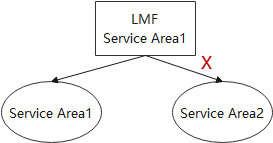


Figure 6.1.1-1

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

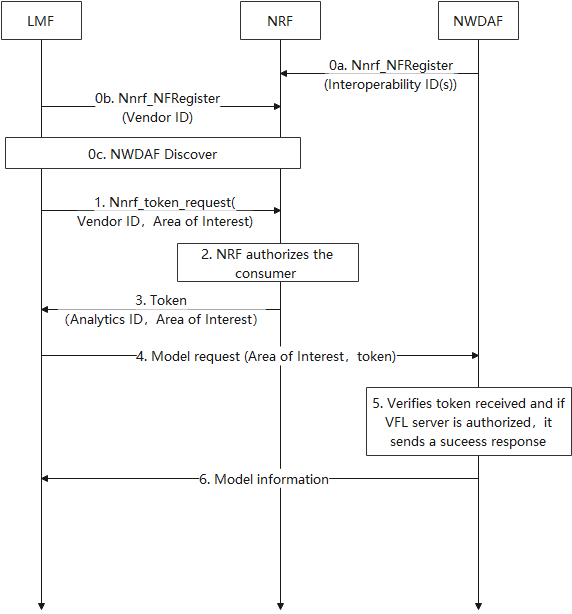


Figure 6.1.2-1 Authorization of AIML model procedure for LMF

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.

### 6.1.3 Evaluation

This solution addresses Key Issue#1 on enhancements to LCS to support AIML by reusing model authorization procedure described in clause X.10 of TS 33.501 [5]. The LCS registers its vendor ID in the NRF, allowing the NRF to authorize the LCS to retrieve model based on the Interoperability indicator. In the assumption of this solution, the LMF is authorized to get the LCS related ML model, whose service area is within the service area registered during the LMF profile registration and validated during access token. Thus, LMF is not allowed to get the UE location information which is out of the service area of the LMF.

## 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.

NOTE: Whether model storage at ADRF is relevant for models to be consumed at the LMF is not clarified.

### 6.2.3 Evaluation

The mechanism defined in Annex X.10 of TS 33.501 [5] is reused to authorize LMF to retrieve the AI/ML model from the NWDAF, in which the LMF is the NF service consumer.

NOTE: Evaluation is not complete.

## 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. NEF can register AF details to NRF via Nnrf\_NFManagement\_Register or Update during the AF connection or when AF provides the capability to 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. supported role (Client, Server)) and interoperability indicator per analytics.

#### 6.3.2.1 AF (VFL Server) requesting the NWDAF



Figure 6.3.2-1 Procedure of authorization of VFL member selection

The consumer 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, additional source (as defined in TS 29.510 [8]), interoperability indicator/vendor Id and target NF's VLF capability for the requested VFL process (Step 2).

The NRF authorises the 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 (Step 3, 4).

Example: If AF is interested in VFL process where AF wants to play a role of VFL Server and wanted NWDAF to become VFL Client, the NEF sends an access token request with source VFL Capability/role= VFL Server, target VFL Capability= VLF Client, target = NWDAF, source = NEF, additional source= AF (as defined in TS 29510 [8]) along with existing IEs. The NRF authorizes the NEF to coordinate on behalf of AF and authorizes AF to run VFL as a VFL server with NWDAF.

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

#### 6.3.2.1 NWDAF (VFL Server) requesting the AF



Figure 6.3.2-2 Procedure of authorization of VFL member selection

The consumer NWDAF/AF sends an access token request to the NRF. The access token request may contain the Analytics ID, source NF, additional target, interoperability indicator/vendor Id and target NF's VLF capability for the requested VFL process.

The NRF authorises the NWDAF/Internal 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 and additional target.

Example: If NWDAF is interested in VFL process where NWDAF wants to play a role of VFL Server and wanted AFs to become VFL Client, the NWDAF sends an access token request with source VFL Capability/role= VFL Server, target VFL Capability= VLF Client, target = NEF, additional target =AF, along with existing IEs. The NRF authorizes the NWDAF to run VFL as a VFL server with NWDAF.

The consumer NWDAF/Internal AF sends the service request, including an access token, to the producer NEF. The producer/NEF verifies the token and allows the VFL procedure with the requested AF.

NOTE: Rational for adding target VFL capability into token and how to verify it is not provided.

### 6.3.3 Evaluation

The solution addresses key issue #2 "Authorization mechanism of selection of VFL participants in the VFL group". It proposes to reuse NRF based authorization that NRF authorizes the VFL service request for the VFL participants based on the registered NF profile information for involving NWDAF and/or External AF.

For the case AF acts as VFL server, AF specific info is registered in NEF as part of NF profile of NEF.

AF (VFL server) triggers VFL service towards NWDAF(VFL client) via NEF. The NEF authorizes the External AF as specified in TS 33.501 [5] clause 12. If External AF is authorized, the NEF request the access token on behave of the External AF(VFL server). The NRF performs authorization check and provides token. I.e. the authorization is based upon the VFL capability and AF specific information provided by the AF(VFL server) during registration, and the VFL related authorization information provided by the NWDAF(VFL client) during registration.

The access token is generated for the NEF (e.g., NEF as subject) and can also include AF specific information. So that when NWDAF(VFL client) receives the VFL service request forwarded by NEF, it can grant VFL service request from AF (VFL server) via NEF based on the token provided by NEF.

## 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

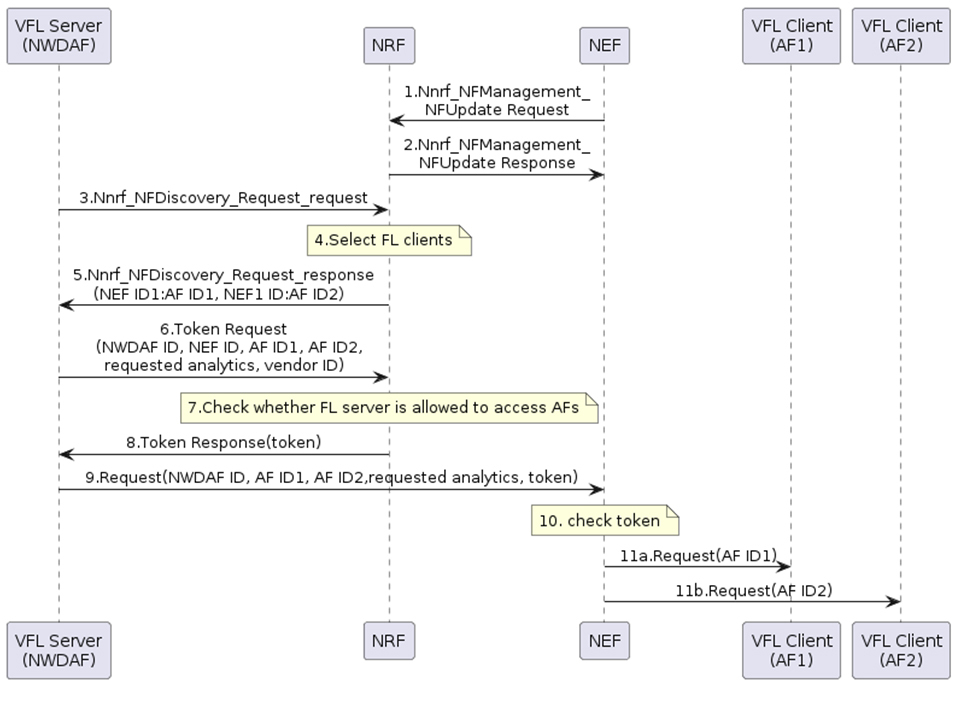


Figure 6.4.2.1-1 Procedure of authorization of VFL member selection (NWDAF is VFL server)

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.

6) 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.

7) 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.

8) The NRF sends token to the NWDAF.

9) 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.

10) 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.

11) After successful checking, the NEF sends request for VFL to different AF.

12) The AF(s) sends response for VFL to the NEF.

NOTE: In step 1, NEF registers external AF information in NRF. In step 4, NRF discovers AF based on the AF information, while NEF does not know the discovered AFs. In step 8, NRF assign token for the NWDAF to access those AFs via NEF. Since information for discovery and authorization are only available on NRF, it is reason why NRF to authorize NWDAF on behalf of external AF.

#### 6.4.2.2 AF is VFL Server

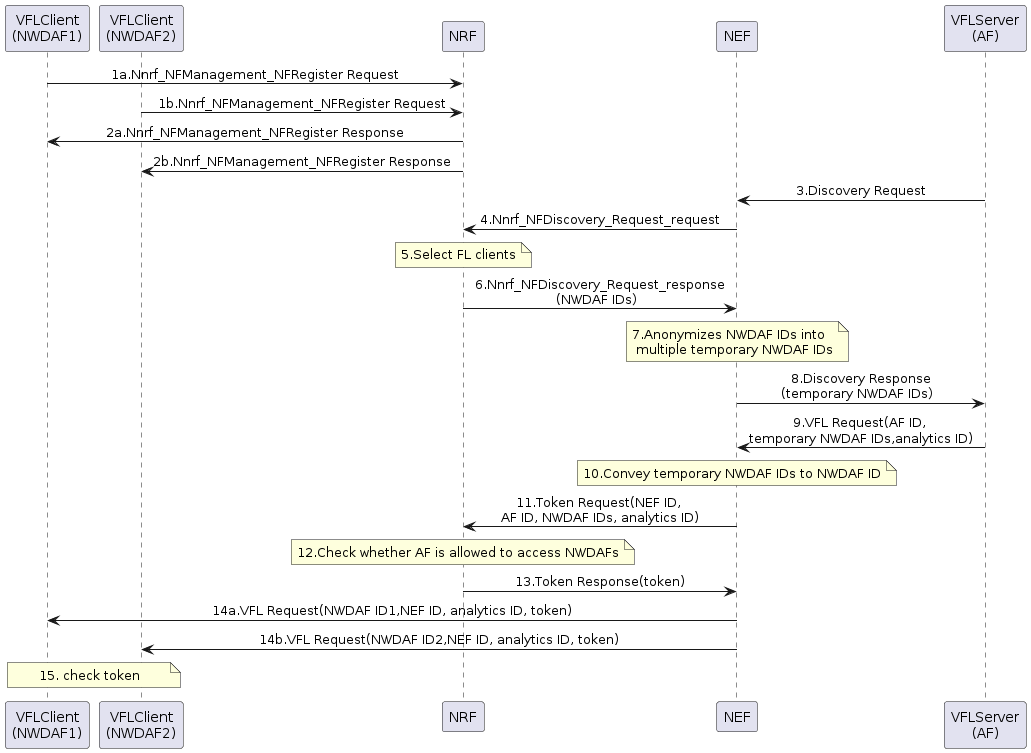


Figure 6.4.2.2-1 Procedure of authorization of VFL member selection (AF is VFL server)

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.

3) When AF (VFL Server) needs to discovery the available NWDAFs for VFL training, the AF sends Discovery Request to NEF.

4) The NEF invokes Nnrf\_NFDiscovery\_Request\_request service operation.

5) The NRF matches the requested query for NWDAFs with the registered NWDAF Profiles. It is assumed that NWDAF ID1 and NWDAF ID2 are selected.

6) The NRF sends Nnrf\_NFDiscovery\_Request\_response message to the NEF. The message includes the selected NWDAF ID1 and NWDAF ID2.

7) 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.

NOTE: When the AF is out of 3GPP domain, the NEF is always involved as outlined in P#2.2.3 of TR 23.700-84 [3]. One of the NEF's functionality is to " handling masking of network and user sensitive information to external AF's according to the network policy" as described in 6.2.5.0 of TS 23.501 [9]. How to handle masking of network and user sensitive information is left to NEF implementation. For example, the NEF can anonymize NWDAF IDs, which masks NWDAF Instance numbers to external entities without necessitating extra signalling.

8) The NEF sends Discovery Response message to the AF including the temporary NWDAF IDs.

9) The AF sends VFL request (e.g. sample alignment request) to the NEF. The request includes AF IDs, temporary NWDAF IDs, and analytics ID.

10) The NEF conveys the temporary NWDAF IDs into NWDAF IDs

11) 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.

12) 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.

13) The NRF sends token to the NWDAF.

14) 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.

15) The NWDAF checks the token, including check integrity of the token, and check whether analytics ID is included in the token.

16) The NWDAF(s) sends response for VFL to the AF.

### 6.4.3 Evaluation

The solution addresses requirement of the key issue #2.

The procedure is aligned with conclusion P#2.2 in TR 23.700-84 [3] which includes both NWDAF is VFL Server case and AF is VFL Server case, especially for untrusted AF case.

The solution uses SBA token based solution for authorization. In addition, in AF is VFL Server case, the NEF can mask NWDAF numbers to the external without involving any additional signalling to meet NEF security requirements that “Internal 5G Core information such as DNN, S-NSSAI etc., shall not be sent outside the 3GPP operator domain” depicted in 5.9.2.3 in TS 33.501 [5].

For case that NWDAF is VFL Server, like NEF subscribes AF profile to the NRF on behalf of the AF, it is proposed that the internal NEF authorizes internal NWDAF to communicate with the external AF on behalf of the external AF. It addresses the security issue of selection of unauthorized VFL client as outlined in key issue#2: it is assumed that the NRF only returns NWDAF with AF clients (e.g. a, b, c) in discovery process. However, the NWDAF may request NEF to initiate VFL with AF clients a, b, c, and d. Without authorization checking on the NEF, the unauthorized AF client d is selected for VFL.

The solution has the following impact:

For NWDAF is VLF server case:

NWDAF: token request and response for assigned token. Vendor ID is included in token request.

NRF: token assignment based on vendor ID and interoperability indicator. The analytics ID and VFL client ID is included in token.

NEF: token check including checking analytics ID and VFL client ID.

For AF is VLF server case:

NEF: NWDAF ID anonymization, token request and response for assigned token.

NRF: token assignment based on vendor ID and interoperability indicator. The analytics ID is included in token.

NWDAF: token check including checking analytics ID.

## 6.5 Solution #5: Authorization of VFL participants involving NWDAF and AF

### 6.5.1 Introduction

This solution addresses Key Issue #2 "Authorization mechanism of selection of VFL participants in the VFL group".

In this solution, the FL Server with VFL capability refers to the NWDAF/External AF that plays the role of the VFL Server, while the FL Client with VFL Capabilities refers to the NWDAF/External AF that plays the role of VFL Client, as defined in TR 23.700-84 [3].

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) and its VFL capability (VFL server) on behalf of the External AF. The NWDAF (VFL client) registers to the NRF with its VFL capability (VFL client) and the authorization information used for VFL procedure, e.g., allowed VFL server (External AF) related information (AF ID).

The NRF then authorizes the VFL service request from AF(VFL server) towards NWDAF(VFL Client) based on the VFL capability type (VFL server) and AF specific information (e.g., AF ID) provided by the AF(VFL server) during registration, and the VFL related authorization information (e.g. a list of allowed AF IDs ) provided by the NWDAF(VFL client) during registration.

When the NWDAF assumes the role of the VFL server and External AF acts as VFL client, whether the External AF provides service to the 5GC and NWDAF to ultilize its capability for FL procedure is upto AF service provider’s policy. Thus authorization of 5GC and NWDAF participating VFL procedure in AF is upto AF’s implemention.

### 6.5.2 Solution details

#### 6.5.2.1 External AF acts as VFL Server



Figure 6.5.2-1: VFL authorization when the External AF acts as a VFL Server

Step 1a. The NWDAF containing MTLF acting as VFL client registers to the NRF with its supported VFL capability (VFL client)and the authorization information used for VFL. It can be a list of AF specific information (e.g., AF ID) that are allowed for VFL.

Step 1b. The External AF sends registration request to the NEF to indicate that it wants to invoke VFL service 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 supported VFL capability (VFL server), AF specific information (e.g., AF ID).

NOTE 1: External AF may register its data via OAM configuration at NEF.

Step 1c. The NEF registers to the NRF within its NF profile about the the AF information as specified in clause 6.2.2.3 of TS 23.288 and includes as part of the information the AF’s VFL related information, including supported VFL capability (VFL server), AF specific information (e.g., AF ID).

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

NOTE 2: The details of how the AF selects candidate NWDAF(s) as VFL client(s) and whether the NF instance ID of NWDAF containing MTLF is sent to external AF is not described in this solution.

Step 3a. The External AF acting as VFL 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 VFL 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 VFL server to perform VFL service request towards the VFL clients. The token request may contain the Analytics ID for the requested VFL process and also AF specific information (e.g., AF ID).

Step 4. NRF checks whether the NF Service consumer (NEF) is authorized to access the requested service in VFL client (NWDAF). In case of the NF Service Consumer (NEF) request VFL service for the External AF acting as VFL server, the NRF also verifies that the AF specific information (e.g., AF ID) is included in the authorization information used for VFL provided by the VFL 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) e.g. AF acting VFL server is as service consumer .

NOTE 3: Fine-grained authorization can be done locally at the NWDAFs containing MTLF acting as VFL client(s). Also, fine-grained authorization can be done locally at the NEF.

NOTE 4: Further role of NEF (e.g. in VFL preparation, sample alignment procedure) is not described in this solution.

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 VFL clients, with the obtained token.

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

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

#### 6.5.2.2 NWDAF acts as VFL Server and external AF as VFL client

Figure 6.5.2.2-1: VFL authorization when NWDAF acts as a VFL Server

Step 1a. The external AF registers its information in the NEF to indicate supported VFL capability (VFL server), AF specific information (e.g., AF ID).

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

Step 1b. The NEF registers the AF to the NRF with its FL related information, including supported VFL capability (VFL client), AF specific information (e.g. AF ID).

Step 1c. The NWDAF containing MTLF registers to the NRF, e.g. its VFL capability (VFL Server) etc.

Step 2. The NWDAF containing MTLF acting as VFL server (NF Service Consumer) discovers other NWDAF(s) and/or AF(s) as VFL Client from NRF by invoking the Nnrf\_NFDiscovery\_Request service operation.

Step 3. The NWDAF containing MTLF acting as FL server (NF Service Consumer) sends an access token request to the NRF as specified in clause 13.4.1 to access NEF service for triggering VFL procedure with external AFs.

Step 4. The NRF checks the NWDAF containing MTLF acting as FL server (NF Consumer) is authorized to access the service provided by NEF to request VFL service from AF, based on the registration information received in Step 1b. If the authorization succeeds, NRF generates the access token(s) as specified in TS 33.501 [5] clause 13.4.1.

Step 5. The NRF sends the access token to the NWDAF containing MTLF acting as FL Server.

Step 6. The NWDAF containing MTLF acting as VFL server sends the VFL service request to the discovered/selected AF (VFL client) via NEF, with the access token received in Step 5. Step 7a, 7b. The NEF verifies the received access token and that the NWDAF containing MTLF (NFc) is authorized to access NEF service to request VFL service from AF. In case of successful access token verification, the NEF sends VFL service request to the AF. Protection of NEF-AF interface is as specified in clause 12 TS 33.501 [5].

Step 8a, 8b. The AF performs authorization of VFL service request based on its local policy and implementation. The AF sends success/failure response to the NEF based on authorization result. The NEF forwards the response to the NWDAF containing MTLF acting as the VFL server.

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

### 6.5.3 Evaluation

The solution addresses key issue #2 "Authorization mechanism of selection of VFL participants in the VFL group". It proposes to reuse NRF based authorization that NRF authorizes the VFL service request for the VFL participants based on the registered NF profile information for involving NWDAF and/or External AF.

For the case AF acts as VFL server, AF specific info is registered in NEF as part of NF profile of NEF.

When AF (VFL server) is to trigger VFL service towards NWDAF(VFL client) via NEF. The NEF authorizes the External AF as specified in TS 33.501 [5] clause 12. If External AF is authorized, the NEF request the access token on behave of the External AF(VFL server). The NRF performs authorization check and provides token that follows the same principle of HFL as specified in Annex X.9 TS 33.501 [5]. I.e. the authorization is based upon the FL capability type and AF specific information (e.g., AF ID) provided by the AF(VFL server) during registration, and the VFL related authorization information provided by the NWDAF(VFL client) during registration (e.g. a list of allowed AF IDs ).

The access token is generated for the NEF (e.g., NEF as subject) and can also include AF specific information. So that when NWDAF(VFL client) receives the VFL service request forwarded by NEF, it can grant VFL service request from AF (VFL server) via NEF based on the token provided by NEF.

For the case NWDAF acts as VFL server and external AF acts as VFL client, the existing SBI token-based authorization is used to authorize NWDAF to invoke VFL procedure towards external AF via NEF, and the existing NEF-AF interface security is used to protect the interaction between NEF and AF for VFL interactions. The external AF performs authorization of VFL service based on its local policy and implementation. The actions of the AF are not defined in 3GPP. This solution does not provide token-based authorization of MNO internal NWDAFs at AF granularity. The reason is that, from the external AF's point of view, the NWDAF and the NRF belong to the same domain, the MNO domain. Which NWDAF acts as server therefore does not matter from the external AF's point of view. From the MNO/PLMN point of view, token-based authorization is provided at NEF granularity.

## 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.

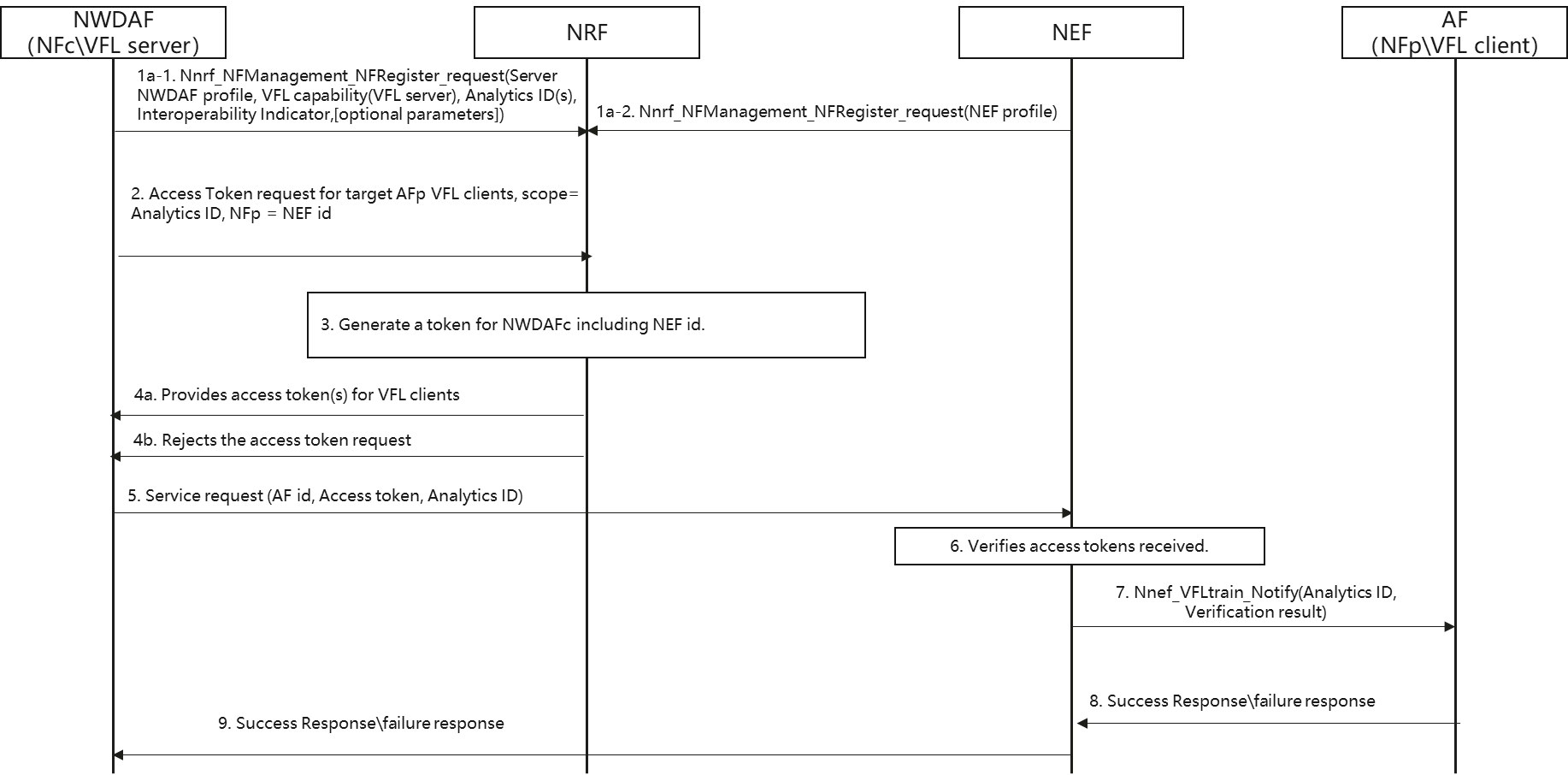


Figure 6.6.2 -1: Authorization mechanism through NRF and NEF for AF outside the PLMN.

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 ID. If the AF is also in the VFL group, the VFL Interoperability ID also includes Application Name or AF Identifier(s).

2) The NWDAF requests an access token from the NRF to be able to consume API service of NEF. 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 and Analytics ID. In addition, optional parameter includes Vendor ID and VFL Interoperability ID.

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). 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 VFL Interoperability ID.

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.

7) In case of successful access token verification, the NEF sends a request to the AF for joining the VFL group. The request contains the Analytics ID and the verification result.

The VFL client (e.g., AF) determines whether to join the network based on the local policy.

8) The AF sends a success response to the VFL server through NEF. Otherwise, the AF sends a failure response.

9) If the NEF receives a success response, the NEF sends a success response to the NWDAF.

### 6.6.3 Evaluation

This solution addresses the requirement of KI#2 to authorize only the trusted VFL members to participate in the FL process within the VFL group including NWDAFs and/or AFs. The solution considers the case of an AF located outside the MNO and deals the authorization aspects of VFL server in the VFL group through NRF and NEF. The procedure proposes to use a token for authorization check when the VFL server sends a service request for a VFL client to join the VFL group through NRF and NEF. The NRF verifies the VFL Interoperability ID in the token request whether it is within the VFL Interoperability ID(s); and the NEF obtains the Analytics ID contained in the access token and verifies whether it is the same as the Analytics ID received from the service request. In case of successful access token verification, the NEF sends a request to the VFL client for joining the VFL group.

The solution has the following impact:

NWDAF: token request and response for generated token. The access token request sent to the NRF includes the NEF ID and Analytics ID, Vendor ID and VFL Interoperability ID.

NRF: the generated token includes the VFL Interoperability ID.

NEF: Token verification including the Analytics ID and AF ID.

## 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 VFL client, the NWDAF can serve as the VFL server, the NWDAF can serve as VFL server as well as VFL 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. VFL client). The request also contains the certificate or CCA (Client Credentials Assertion) of the AF.

NOTE: Reason for need to use CCA for external AF to participate in the VFL group is not provided.

2.The NEF authorizes the AF to trigger the service based on the local policy or OAuth 2.0.

3.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.

4.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. The Intention of using CCA is to enable the NRF to check if the AF identifier in the token request is originally triggered by the AF that owns the AF identifier. The verifying of the CCA/certificate of the AF requires that the cross-certification process is established between the network domain and AF domain.

5.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.

6.The NEF sends the received NWDAF identifier(s) to the AF.

7.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.

8.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.

NOTE: Identify information, i.e. NWDAF instance ID is not protected in this solution.

9.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.

10.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).

11.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.

12.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 AF's CCA/certificate. The Intention of using CCA is to enable the NRF to check if the AF identifier in the service request is originally triggered by the AF that owns the AF identifier. The verifying of the CCA/certificate of the AF requires that the cross-certification process is established between the network domain and AF domain.

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.

13.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.

14.The NEF sends federated learning related response (e.g., sample information including UE ID) to the AF.

### 6.7.3 Evaluation

This solution partly addresses KI#2 requirement of authorization of members involved in vertical federated learning (VFL) group, where the AF out of 3GPP operator domain is the VFL server.

In this solution, NRF leverages the NWDAF's NF profile to authorize AF to request NWDAF to provide federated learning related services.

NEF requests token from the NRF on behalf of the AF, in which the token is used to authorize the AF to request federated learning service of NWDAF. The token generated by the NRF includes the AF identifier and the token's subject claim is the NEF's NF instance ID.

NEF requests NWDAF's federated learning service on behalf of the AF, in which the token includes the AF identifier and the token's subject claim is the NEF's NF instance ID.

In this solution, NRF/NWDAF uses CCA/certificate to check if the AF identifier in the message is triggered by the AF out of 3GPP operator domain. The using of CCA/certificate needs the cross-certificate procedure among PLMN NFs and the AF, which is not support by the current 3GPP system.

NOTE: Evaluation is not complete.

## 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.

0.AF registers its profile to the NRF via the NEF.

1.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 VFL capability information (i.e., AF can serve as the VFL client or the AF can serve as VFL server as well as VFL 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).

NOTE: Motivation for NRF to authorize the NWDAF to access services of external AF is not provided.

2.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 VFL capability of the AF, the federated learning Model supported by the AF.

3.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.

4.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 VFL capability (i.e., AF can serve as the VFL client or the AF can serve as VFL server as well as VFL client) of the AF, 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).

5.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. VFL capability of the AF, 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.

6.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.

7.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.

8.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.

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

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

### 6.8.3 Evaluation

This solution partly addresses the KI#2 requirement of authorization of members involved in vertical federated learning (VFL) group, where NWDAF is the VFL server.

In this solution, the NEF profile for AF out of 3GPP operator domain is used to authorize NWDAF to select untrusted AF to serve as VFL client. The NRF shall store the VLF capability of untrusted AF in the NEF NF profile.

To enable NWDAF to request service from AF via the NEF, the AF identifier is included in the token generated by the NRF. And the NEF's NF instance ID is set as the token's audience claim.

NOTE: Evaluation is not complete.

## 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).

In case of external AF as VFL server, the NEF is to assist the AF as VFL Server handle VFL sample alignment.

In case of NWDAF as VFL server, the NWDAF as VFL Server handles sample alignment and optionally assigns new VFL sample ID(s) for the overlapped sample ID(s). It is helpful for VFL entities to improve the efficiency of VFL when doing VFL, for example, avoid sample ID mapping in the VFL for the NEF. The terminology described is the following:

VFL Group ID: Vertical Federal learning Group Identifier represents the Vertical Federal learning capability group. Each VFL entities can support multiple VFL Group ID(s). Entities sharing the same VFL Group ID can collaborate in VFL tasks. These IDs could be pre-configured by the OAM, and each VFL entities shall register its supported VFL Group ID(s) in the NRF. For example, entity A support VFL Group ID (ID1, ID2, ID3), entity B support VFL Group ID (ID2), and entity C support VFL Group ID(ID3), then Entity A can collaborate with Entity B using ID2 and with Entity C using ID3. However, Entities B and C cannot collaborate as they do not share a common VFL Group ID.

NOTE1: The alignment with the stage 2 work of VFL Group ID used in this solution is not addressed in the present document..

Sample ID: The Identifier of Sample, represents the data used in the local VFL task. The Sample ID can be UE ID (e.g. SUPI, GPSI) or IP address, and so on.

VFL Sample ID: This identifier is used in the VFL task to ensure consistency and unnecessary exposure of the UE ID across different VFL AF members. When the Sample ID is a UE ID, it may vary across different VFL AF members. To streamline the process, the CN can assign a new VFL Sample ID so that all VFL entities use the same ID for the sample. For instance, if AF1 supports sample IDs (AF1 UE ID1, AF1 UE ID2) and AF2 supports sample IDs (AF2 UE ID1, AF2 UE ID2), after sample alignment, the common sample IDs are UE1 and UE2. The corresponding VFL Sample IDs for these samples will be VFL UE ID1 and VFL UE ID2.

NOTE 2: The VFL Sample ID is only used in this solution.

|  |  |  |  |
| --- | --- | --- | --- |
|  | AF1 | AF2 | VFL sample ID |
| UE1 | AF UE ID1 | AF2 UE ID1 | VFL UE ID1 |
| UE2 | AF UE ID2 | AF2 UE ID2 | VFL UE ID2 |
| UE3 | AF UE ID3 |  |  |

### 6.9.2 Solution details

#### 6.9.2.1 Sample alignment procedure for Vertical Federated Learning when NWDAF is acting as the VFL server



Figure 6.9.2.1 Sample alignment procedure for Vertical Federated Learning when NWDAF is acting as the VFL server

0a-0. The VFL entities (e.g., VFL Server, VFL Client) register its supported VFL Group ID(s).

1. The NWDAF as VFL Server discoveries the VFL Clients(e.g, NWDAF(s) as VFL Client, AF(s) as VFL Client) via NRF by invoking the NF discovery.

2. The NWDAF as VFL Server sends sample alignment request to the VFL Clients including the VFL Group ID, analytics ID(s) and VFL capability type(i.e, VFL Client).

3. The VFL Clients return the supported Sample ID(s).

4. The NWDAF as VFL Server generates the final intersection of the Sample ID(s) based on received results in step 3 and local supported Sample ID(s). If the sample ID(s) received in step3 is GPSI(s), the Server could map the GPSI into SUPI to generates the final intersection of the sample ID. The Server may assign VFL sample ID(s). The VFL sample ID(s) are new sample ID(s) for the intersection of sample ID(s) which is same among all VFL members.

5. The NWDAF as VFL server returns the final intersection sample ID(s) and VFL sample ID(s) to the VFL Client(s).

6. All VFL entities determine the overlapped VFL sample ID(s).

#### 6.9.2.2 Sample alignment procedure for Vertical Federated Learning when External AF is acting as the VFL server



Figure 6.9.2.2 Sample alignment procedure

0a-0. The VFL entities (e.g., VFL Server, VFL Client) and NEF register its supported VFL Group ID(s).

1. The AF as VFL Server discoveries the VFL entities(e.g, NWDAF as VFL clients) via NRF by invoking the NF discovery through NEF.

2. The AF as VFL Server sends sample alignment request to the NEF including the VFL Group ID and VFL entities and the Sample space, which includes the list of Sample IDs to be considered for VFL Training.

3. The NEF cache’s the set of the sample space received in step 2. The NEF sends VFL sample information request to each VFL entities received in the step2.

5.. VFL entities return the supported sample ID(s) to the NEF.

NOTE: How VFL Participants determine the returned sample ID(s) is not addressed in the present document.

6. The NEF determines the common sample ID(s) list based on received results in step 2 and step 5. If the Sample ID(s) in step2 is external UE ID(GPSI), the NEF may map the external UE ID to the Internal UE ID(SUPI).

7. The NEF returns the common sample ID(s) list to the VFL Server.

8. The AF as VFL Server then determines the final intersection of the Sample ID(s) based on the results received by NEF in step 7.

9. The AF as VFL Server returns the determined Sample ID(s) to the VFL Client(s).

10. All VFL entities determine the overlapped VFL sample ID(s).

NOTE: How to perform sample alignment is described in TS 23.288 [7].

### 6.9.3 Evaluation

This solution addresses key issue #3, focusing on the privacy concerns in Vertical Federated Learning (VFL) among VFL members, particularly during the sample alignment phase. In case of the AF as VFL Server, it proposes introducing NEF to handle sample alignment. This ensures that external AF as VFL Server only access overlapping sample information. In case of NWDAF acts as VFL server, the NWDAF as VFL Server handles sample alignment and assigns VFL Sample ID(s) for the intersection of Sample ID(s) and provides to VFL Clients.

## 6.10 Solution #10: Privacy of 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 to reduce the exposed sample and sends reduced sample list to the VFL server to do final decision so that the external AF will not know internal sample ID list.

### 6.10.2 Solution details

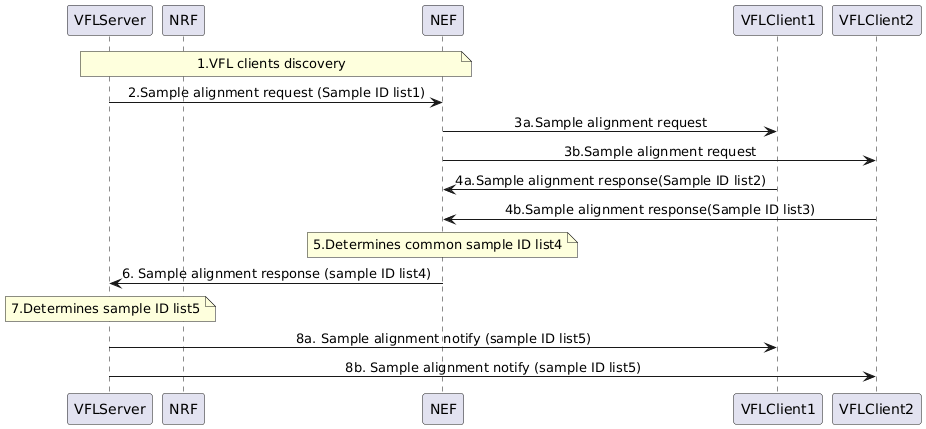


Figure 6.10.2-1 Procedure of Privacy of sample alignment

1) VFL Server has already completed VFL clients discovery.

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

2) 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).

3) NEF sends Sample alignment request to the VFL clients in the same VFL group.

4) VFL Clients reply Sample alignment response to the NEF. The Sample alignment response includes sample ID list 2 and 3.

5) 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.

6) The NEF sends sample alignment response message to VFL server including the common sample ID list 4.

7) The VFL Server determines sample ID list 5 based on the received common sample ID list 4. The VFL Server may narrow down the sample ID list.

8) The VLF Server sends sample alignment notify message to the VFL Clients (via NEF), the determined sample ID list 5 will be included. The sample ID list 5 will be the final sample ID list.

### 6.10.3 Evaluation

The solution addresses the key issue #3.

The solution proposes to use NEF to do sample alignment to reduce the exposed sample and sends reduced sample list to the VFL server to do final decision so that the external AF will not know internal sample ID list.

Where the AF is acting as a server and NWDAF as a client, it is essential to understand the risk that can emerge during sample alignment if this process is left out for AF which is out of the 3GPP operator domain. This would potentially reveal unnecessary UEID to the external AF which may lead to regulatory violations in certain cases.

To mitigate such circumstances NEF which operates at the edge of the operator's network, can narrow down sample IDs the external AF (when server). By acting as an intermediary, the NEF ensures that UEID are not unnecessarily revealed to the external AF during the sample alignment. The NEF can map the internal UEID to external and vice versa before sharing them with the external AF and generate the interclause of the samples that can be used in the training process, thereby protecting user identities.

NOTE: the role of NEF in VFL depends on TS 23.288 [7] and whether there is a need to have GPSI to SUPI conversion by NEF is not provided.

## 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.

NOTE: Whether the conversion between internal UE ID to external UE ID is needed is not provided.

NOTE: How to perform sample alignment is described in TS 23.288 [7].

#### 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 before forwarding the VFL service request.

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

Step 4. If external UE IDs are received in step 3, the NEF performs external UE IDs mapping to internal UI IDs (SUPI).

Step 5. The NEF forwards the VFL service response.

Step 6. 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 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.

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

Step 4. If internal UE IDs (SUPI) have been received in Step 3, the NEF performs mapping of internal UE IDs (SUPI) to external UE IDs.

Step 5. The NEF forwards the VFL Service Response.

Step 6. The Vertical Federated Learning procedure is performed between FL server (NWDAF) and FL client (AF) via the NEF.

### 6.11.3 Evaluation

NOTE: Evaluation is not complete.

## 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 server (i.e. NWDAF) and 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 VFL server triggers the VFL operation with one or more AFs as the 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, optionally including the candidate samples (i.e. internal UE IDs) and feature profiles the NWDAF wants to use for the VFL training.

2.[Optional] 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 client AFs:

4.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).

5.The AF sends the VFL sample and feature alignment response to the NEF, including selected external UE ID and feature profiles.

6.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 may select the intersection of UE IDs in these responses.

7.The NEF sends the VFL sample and feature alignment response to the NWDAF, including the internal UE ID and feature profiles.

8.The NWDAF as VFL server will determine the final list of samples from the intersection of candidate sample lists chosen by AF(s).

9.The NWDAF may send the VFL sample and feature alignment notify to the AF(s) through NEF, including the external ID and optional feature profiles of samples.

NOTE 1: Feature alignment is optional in this solution.

NOTE 2: This solution assumes that the VFL Sample ID is UE ID i.e., internal UE ID or external UE ID, and VFL Sample IDs vary across VFL participant AF(s) and NWDAF(s).

### 6.12.3 Evaluation

This solution addresses the security requirement of KI #3, which relies on the NEF with mapping of information of UE IDs to be involved in the VFL sample alignment initialled by the NWDAF.

Features alignment and use of the features are made optional in the VFL process in the conclusion of KI#2 P.2.3 of TR 23.700-84 [3]. How the features are registered and whether feature alignment is supported in the sample alignment is an early call. Hence limiting this to sample alignment only should be considered.

## 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.

NOTE: How to enable privacy protection for AF initiated federated learning is not provided.

### 6.13.3 Evaluation

NOTE: Evaluation is not complete.

## 6.14 Solution #14: Authorization for LCS Data Storage and Retrieval

### 6.14.1 Introduction

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

As outlined in Principles #1 and #3.3 of clause 8.1 in TR 23.700-84 [3], the AI/ML model training entity (e.g., an NWDAF containing an MTLF) can obtain training data for AI/ML-based positioning from data sources such as the data source (e.g. LMF) and/or ADRF. When collecting data from ADRF, a DataSetTag or Storage Transaction ID can be used to identify the data set. However, since the AI/ML model training entity may be different from the data sources, there is a risk that an unauthorized or misused NWDAF containing MTLF could obtain training data corresponding to the DataSetTag or Storage Transaction ID. Therefore, additional protection measures should be considered to prevent data leakage.

This solution applies a principle similar to that described in clause X.10, "Security for AI/ML model storage and sharing," of TS 33.501 [5], to address the authorization issue in KI#1 to ensure the training data will not leaked to the unauthorized entities.

### 6.14.2 Solution details



Figure 6.14.2-1: Secured and authorized training data sharing

1. [Optional] The data source (e.g. LMF) may send data storage request to store the training data related to the model training for AI/ML based positioning in ADRF by using Nadrf\_Data\_Managment\_Storage Request, which includes data source ID, training data, and optional DataSetTag and allowed NF list as defined in clause 6.2B.2 of TS 23.288 [7].

2. [Optional] The ADRF sends the response to the data source with the DataSetTag or a Storage Transaction ID if the DataSetTag is not included in step 1.

3. [Optional] Data consumer, e.g., NWDAF containing MTLF, may perform Nnrf\_NFDiscovery\_Request operation to select a suitable Data Producer, e.g., data source.

4. The Data consumer sends the vendor ID, target NF (e.g. LMF), the service to be used for requesting data, and optional data type to NRF to request an access token for obtaining the data from the data source using the Nnrf\_AccessToken\_Get request operation as defined in TS 33.501 [5].

5. The NRF checks whether the data consumer is authorized to access the requested service and the request data type in data source and grants the token (token1). The token1 includes the requested service and the request data type.

6. The Data consumer sends a request to obtain the training data for model training with token1, its NF instance ID and optional data type to specify the requested data.

7. The data source verifies the access token as specified in the clause 13.4.1.1.2 of TS 33.501 [5]. If verification is successful, the data source determines the data to be shared for model training and stored the NF instance ID of Data consumer as part of allowed NF instance list.

8-9. [Optional] In case that the training data is stored in ADRF, if NF consumer is not in the allowed NF list, the data source shall send data storage request to ADRF to update the allowed NF list.

10a. In case that the training data is stored in ADRF, the data source sends the response to the Data consumer with ADRF ID, DataSetTag or Storage Transaction ID.

10b. In case that the training data is not stored in ADRF, the data source sends the response to the Data consumer with the training data.

11-12. If step 10a is received, the Data consumer requests an access token 2 for obtaining the data from the ADRF using the Nnrf\_AccessToken\_Get request operation as defined in TS 33.501 [5].

13. Data consumer requests to retrieve the target data by sending Nadrf\_DataManagement\_Retrieval Request as described in TS 23.288 [7], including token2.

14. ADRF verifies the access token (token2) as specified in the clause 13.4.1.1.2 TS 33.501 [5]. ADRF also verifies the Data consumer’s NF ID is included in the allowed NF instance list. If verification is successful, ADRF sends Nadrf\_MLModelManagement\_Retrieval Response to the Data consumer with the training data.

NOTE: The alignment with stage 2 work is not addressed in the present document..

### 6.14.3 Evaluation

The solution applies a principle similar to that described in clause X.10 of TS 33.501 [5] to addresses key issue #1.

## 6.15 Solution #15: Reuse the existing SBA mechanisms for protection of communication data in VFL training process.

### 6.15.1 Introduction

The solution addresses the key issue #4.

The solution proposes to reuses the existing SBA mechanisms to protect confidentiality and integrity of communication data used in VFL training process.

### 6.15.2 Solution details

Generally, existing mechanisms of service-based architecture as specified in TS 33.501 [5] (e.g., protection of the NEF – AF interface mechanism described in clause 12.3, protection at the network or transport layer described in clause 13.1) can support integrity protection, anti-replay protection and confidentiality protection for communication between VFL participants, while the NWDAF or the AF acts as VFL server with one or multiple NWDAF(s) or AF(s) act as VFL client(s). The support of TLS is mandatory. Security profiles for TLS implementation and usage follows the provisions given in clause 6.2 of TS 33.210 [10].

### 6.15.3 Evaluation

The solution reuses Clause 12.2 and Clause 12.3 of TS 33.501 [5] without further standards impact.

## 6.16 Solution #16: LMF authorization for AI/ML model retrieval from NWDAF containing MTLF

### 6.16.1 Introduction

The proposed solution addresses the security requirement of key issue #1. The security requirement states: "If AI model training entity and AI model consumer are different, 5GS shall support authentication and authorization of AIML model or training data retrieval between LMF and NWDAF." In addition, the requirement has a NOTE stating: "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.". The proposed solution reuses the principles in Annex X.10 with the difference that LMF is the entity retrieving the model from NWDAF containing MTLF, and that model storage in the ADRF is not applicable.

### 6.16.2 Solution details

The solution is shown in Figure 6.16.2-1.



**Figure 6.16.2-1: LMF authorization for AI/ML model retrieval from NWDAF**

The solution includes the following steps:

0a. NF Service producer, i.e. NWDAF containing MTLF, registers its NF profile in the NRF with ML model interoperability indicator per new indication.

0b. NF service consumer, i.e. LMF, registers at the NRF including its Vendor ID and a new indication.

1. NF Service consumer, i.e. LMF, performs Nnrf\_NFDiscovery\_Request operation

2a. NF Service consumer, i.e. LMF, requests an access token from the NRF using the Nnrf\_AccessToken\_Get request operation. The token request message contains, besides the parameters described in clause 13.4.1.1.2, the Vendor ID of the NF Service consumer and the new indication.

2b. NRF checks whether the NF service consumer is authorized to access the requested service in NWDAF containing MTLF. The NRF verifies that the NF Consumer's Vendor ID is included in the NF Service Producer's interoperability indicator for the new indication. If the authorization is successful, the NRF grants the token including the new indication as specified in the clause 13.4.1

3. NF Service consumer performs Nnwdaf\_MLModelProvision Request (new indication, Vendor ID and token) service operation at the NWDAF containing MTLF to retrieve ML models for the new indication.

4. The NF Service Producer authenticates the NF Service Consumer and verifies the access token as specified in the clause 13.4.1.1.2 and ensures that the new indication is included in the access token. If verification is successful, NWDAF containing MTLF determines the ML model to be shared for the requested new indication.

5. NWDAF containing MTLF sends Nnwdaf\_MLModelProvision Response to the NF Service Consumer with Model ID, the address of the determined ML model.

### 6.16.3 Evaluation

The proposed solution reuses the defined principles in Annex X.10 of TS 33.501[5] to authorize LMF to retrieve AI/ML from NWDAF. In this solution, the LMF is the NF Service consumer, and the AI/ML model is retrieved directly from the NWDAF, not from the ADRF; thus, the AI/ML model storage and sharing in ADRF is not included in the solution.

## 6.17 Solution #17: Privacy of VFL between VFL members

### 6.17.1 Introduction

This solution addresses key issue #3 " Privacy of VFL between VFL members ".

According to the KI#4, vertical federated learning (VFL) allows the interaction of multiple NWDAF(s) and/or AF(s) to cooperate to train models locally where no raw data need to be exchanged. 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.

If the privacy is not protected properly, the UE ID privacy may be leaked during training or in the intermediate model.

Therefore, the KI#3 requirement is that the 5GS shall support privacy protection on sample alignment procedure.

### 6.17.2 Solution details

For privacy protection purpose, the sample ID such as UE ID in the data to VFL model training is anonymized. For VFL training, all feature in VFL participants need to map the internal/external sample ID such as UE ID in different protocol layers (such physical layer, mac layer, application layer, etc) to the same anonymized UE ID used for the VFL sample alignment procedure.

#### 6.17.2.1 General procedures



Figure 6.17.2.1-1 The VFL training data privacy protection

Step 1. VFL participant selection. After the VFL AF selects the VFL participants, the VFL participants are configured with the VFL parameters such as VFP model ID, attributes from each VFL participants, training/inference data processing procedure, VFL server ID, etc. The VFL client and the server determine the common sample space, i.e., the common sample ID set from all the VFL participants.

NOTE 1: Sample space’s predetermination before the sample alignment is not aligned with TS 23.288 [7].

Step2. Sample alignment and mapping internal/external sample ID using information from UDM/UDR, provisioned mapping info from AF, etc and generate one anonymous ID for each Sample ID to protect the privacy during VFL procedure. The mapping information is stored in the NEF to be available in the VFL process.

Step 3. Internal/external sample ID is mapped to the anonymous ID using NEF mapping information before performing the VFL procedure using mapped anonymous sample ID.

NOTE 2: The mapping of UE ID at the NEF is not aligned with TS 23.288 [7].

### 6.17.3 Evaluation

NOTE: Evaluation is not complete.

# 7 Conclusions

## 7.1 Conclusion on Key Issue #1

For Key Issue#1, it is recommended to use the following principles as the baseline for enhancements to LCS to support AIML:

- The LMF shall register its vendor ID in the NRF, allowing the NRF to authorize the LMF to retrieve model based on the interoperability indicator and the indication of supporting model training for LMF-based AI/ML Positioning of NWDAF.

- The LMF utilizes a new indication to indicate retrieval of AI/ML model for LMF-based AI/ML positioning. Therefore, the LMF may include the indicator in the access token request and the NRF may include the same indicator in the access token.

NOTE: Whether new indication can be applied to NWDAF can be discussed in normative work, considering stage-2 outcome.

Regarding user consent aspect for LMF-based AI/ML model positioning, it is concluded that Annex V of TS 33.501 [5] will be re-used as done in TS 23.288 [7]; thus, there is no normative work required.

## 7.2 Conclusion on Key issue #2

In case that external AF is VFL Server, and NWDAF(s) are VFL client(s) (NEF is involved), the following principles for authorization of participant NWDAF(s) for vertical federated learning are recommended for normative work:

1) The NEF includes requested analytics ID and AF ID in token request to NRF. The NRF checks whether the server AF is authorized to access the client NWDAF(s) for this Analytics ID. If the server AF is authorized, the NRF will issue an access token to the NEF. The NEF uses the access token to communicate with client NWDAF(s), and the NWDAF(s) verifies the access token, after successful verification, the NWDAF allows server AF’s request from the NEF.

2) The NRF uses the information included in token request and registered information for the authorization.

In case that NWDAF is VFL Server, and external AF(s) are VFL client(s) (NEF is involved), the following principles for authorization of participant AF(s) for vertical federated learning are recommended for normative work:

1) The server NWDAF includes requested analytics ID and optionally client AF ID(s) in token request to NRF. The NRF checks whether the server NWDAF is authorized to access the NEF for this Analytics ID. If the server NWDAF is authorized, the NRF will issue an access token to the server NWDAF. The server NWDAF uses the access token to communicate with NEF, and the NEF verifies the access token, after successful verification, the NEF allows NWDAF’s request to external client AF(s).

2) The NRF uses the information included in token request and NF profile for the authorization.

3) Authorization of the AF is performed at the NEF, following clause 12 of TS 33.501 [5].

4) The AF may use local policy to authorize VFL service request from NEF and not specified in 3GPP.

1. Additionally, the access token may include the AF ID(s) and Analytics ID, and NEF may check whether the server NWDAF is allowed to access the requested AF based on the access token..

In case that NEF is involved, the following principles for masking internal network information for VFL are recommended for NEF security requirements:

- NF instance ID should not be transmitted outside the 3GPP operator domain via NEF.

## 7.3 Conclusion on Key Issue #3

For Key Issue#3, it is recommended to use the following principles as the baseline, NEF is used to improve privacy between VFL participants during the sample alignment procedure. The NEF can be responsible for performing UE ID mapping, converting internal UE IDs (e.g., SUPI) to external UE IDs.

NOTE: Further potential security and privacy issue is left for the normative phase.

## 7.4 Conclusion on Key issue #4

For Key Issue#4, it is recommended to use the following principles as the baseline that will reuse already established SBA mechanisms as defined in clauses 12.2 and 12.3 of TS 33.501 [5] for the NEF-AF interface and 13. 1 of TS 33.501 [5] for communication among VFL participants. The adoption of these clauses does not instate any impact on the standards. Therefore, no normative work is needed for this key issue.

Annex A:  
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 |
| 2024-08 | SA3#117 | S3-243392 |  |  |  | S3-242807, S3-242840, S3-243078, S3-243191, S3-243246, S3-243647, S3-243575, S3-243576, S3-243577, S3-243578, S3-243579, S3-243580, S3-243581, S3-243582, S3-243583, S3-243584, S3-243585, S3-243586, S3-243587, S3-243588, S3-243589, S3-243590, S3-243591, S3-243592, S3-243593, S3-243594, S3-243595, S3-243596, S3-243597, S3-243704, S3-243705, S3-243713 | 0.3.0 |
| 2024-10 | SA3#118 | S3-243832 |  |  |  | S3‑243894, S3‑243961, S3‑244085, S3‑244233, S3‑244438, S3‑244439, S3‑244440, S3‑244441, S3‑244442, S3‑244443, S3‑244444, S3‑244445, S3‑244446, S3‑244447, S3‑244448, S3‑244495, S3‑244499, S3‑244500, S3‑244514, | 0.4.0 |
| 2024-11 | SA3#119 | S3-245197 |  |  |  | S3-245346, S3-244739, S3-244873, S3-244874, S3-244987, S3-244988, S3-244994, S3-245269, S3-245270, S3-245271, S3-245345, S3-245347 | 0.5.0 |