|  |
| --- |
| 3GPP TR 33.784 V0.1.0 (2024-04) |
| Technical Report |
| 3rd Generation Partnership Project;Technical Specification Group Services and System Aspects;Study on security aspects of Core Network Enhanced Support for AIML (Release 19) |
|   |
|  |  |
| The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP.The present document has not been subject to any approval process by the 3GPPOrganizational Partners and shall not be implemented.This Specification is provided for future development work within 3GPPonly. The Organizational Partners accept no liability for any use of this Specification.Specifications and Reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices. |

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

Contents

Foreword 4

1 Scope 6

2 References 6

3 Definitions of terms, symbols and abbreviations 6

3.1 Terms 6

3.2 Symbols 7

3.3 Abbreviations 7

4 Overview 7

5 Key issues 7

5.1 Key Issue #1: Security aspects on enhancements to LCS to support AIML 7

5.1.1 Key issue details 7

5.1.2 Threats 7

5.1.3 Potential security requirements 7

5.2 Key Issue #2: Authorization mechanism of selection of VFL participants in the VFL group 8

5.2.1 Key issue details 8

5.2.2 Security threats 8

5.2.3 Potential security requirements 8

5.3 Key Issue #3: Privacy of VFL between VFL members 8

5.3.1 Description 8

5.3.2 Security threats 9

5.3.3 Potential security requirements 9

5.X Key Issue #X: <Key Issue Name> 9

5.X.1 Key issue details 9

5.X.2 Threats 9

5.X.3 Potential security requirements 9

6 Solutions 9

6.Y Solution #Y: <Solution Name> 9

6.Y.1 Introduction 9

6.Y.2 Solution details 9

6.Y.3 Evaluation 9

7 Conclusions 9

Annex <X> (informative): Change history 10

# Foreword

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

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

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

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

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

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

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

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

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

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

**should** indicates a recommendation to do something

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

**may** indicates permission to do something

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

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

**can** indicates that something is possible

**cannot** indicates that something is impossible

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

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

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

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

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

In addition:

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

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

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

# 1 Scope

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

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

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

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

# 2 References

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

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

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

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

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

[2] 3GPP TR 38.843: "Study on Artificial Intelligence (AI)/Machine Learning (ML) for NR air interface".

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

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

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

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

## 3.1 Terms

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

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

## 3.2 Symbols

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

<symbol> <Explanation>

## 3.3 Abbreviations

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

<ABBREVIATION> <Expansion>

# 4 Overview

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

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

# 5 Key issues

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

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

### 5.1.1 Key issue details

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

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

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

### 5.1.2 Security Threats

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

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

### 5.1.3 Potential security requirements

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

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

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

### 5.2.1 Key issue details

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

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

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

### 5.2.2 Security threats

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

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

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

### 5.2.3 Potential security requirements

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

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

Editor’s Note: The security issue of potential topology information exposure (e.g. NF instance ID) to external AF after authorization is ffs.

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

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

### 5.3.1 Description

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

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

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

### 5.3.2 Security threats

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

### 5.3.3 Potential security requirements

5GS shall support privacy protection on sample alignment procedure.

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

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

### 5.X.1 Key issue details

### 5.X.2 Threats

### 5.X.3 Potential security requirements

# 6 Solutions

Table 6.0-1: Mapping of solutions to key issues

|  |  |
| --- | --- |
|  | Key Issues |
| **Solutions** | 1 | 2 | 3 | 4 | 5 | X |
| 1 |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |
| X |  |  |  |  |  |  |

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

### 6.Y.1 Introduction

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

### 6.Y.2 Solution details

### 6.Y.3 Evaluation

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

# 7 Conclusions

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

Annex <X> (informative):
Change history

|  |
| --- |
| **Change history** |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2024-04 | SA3#115Adhoc-e | S3-241287 |  |  |  | TR skeleton for TR 33.784 | 0.0.0 |
| 2024-04 | SA3#115Adhoc-e | S3-241651 |  |  |  | S3-241290, S3-241621, S3-241639, S3-241615, S3-241624 | 0.1.0 |