|  |
| --- |
| 3GPP TR ab.cde V0.1.0 (2025-08) |
| Technical Report |
| 3rd Generation Partnership Project;Technical Specification Group Services and System Aspects;Study on AIML Enablement Service Security(Release 20) |
|   |
|  |  |
|  |
| 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 16Internethttps://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.© 2025, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).All rights reserved.UMTS™ is a Trade Mark of ETSI registered for the benefit of its members3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersLTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersGSM® and the GSM logo are registered and owned by the GSM Association |

Contents

Foreword 5

1 Scope 7

2 References 7

3 Definitions of terms, symbols and abbreviations 7

3.1 Terms 7

3.2 Symbols 7

3.3 Abbreviations 8

4 Key Issues 8

4.1 Key Issue #1: Authorization for AIMLE Service Security for FL members 8

4.1.1 Key issue details 8

4.1.2 Security threats 8

4.1.3 Potential security requirements 8

4.2 Key Issue #2: Secure AIMLE ML Model Access 8

4.2.1 Key Issue details 8

4.2.2 Security threats 9

4.2.3 Potential security requirements 9

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

4.X.1 Key Issue details 9

4.X.2 Security threats 9

4.X.3 Potential security requirements 9

5 Solutions 9

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

5.Y.1 Introduction 9

5.Y.2 Solution details 9

5.Y.3 Evaluation 9

6 Conclusions 9

6.Z Key Issue #Z: <Key Issue Name> 9

Annex <A>: <Informative annex title for a Technical Report> 10

Annex <X>: Change history 11

# 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 has the following objectives:

* Identify and study the authentication and authorization aspects for AIMLE services specified in TS 23.482 [3].
* Study the solutions to address the identified scenarios to support AIMLE service security.

NOTE 1: For the above objectives existing SEAL security aspects [2] need to be taken into account as SEAL architecture is used as baseline for the AIMLE architecture. As the AIMLE phase 2 study progress in SA6 [4], related progress can be taken into account when stable conclusion in SA6 is available if any security aspects need to be considered additionally for this security 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 TS 33.434, "Security aspects of Service Enabler Architecture Layer (SEAL) for verticals".

[3] 3GPP TS 23.482, "Functional architecture and information flows for AIML Enablement Service".

[4] 3GPP TR 23.700-83, "Study on application layer support for AI/ML services Phase 2".

…

[x] <doctype> <#>[ ([up to and including]{yyyy[-mm]|V<a[.b[.c]]>}[onwards])]: "<Title>".

# 3 Definitions of terms, symbols and abbreviations

## 3.1 Terms

For the purposes of the present document, the terms given in 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 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 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 TR 21.905 [1].

<ABBREVIATION> <Expansion>

# 4 Key Issues

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

## 4.1 Key Issue #1: Authorization for AIMLE Service Security for FL members

### 4.1.1 Key issue details

3GPP TS 23.482[3] introduces support for AIMLE services, enabling AI/ML operations through interactions between the AIMLE client and AIMLE server(s) over the AIML-UU reference point. These services involve distributed AI/ML operations across multiple participants, necessitating robust security mechanisms to ensure that only authorized members participate in the AIMLE workflows. Given the critical role of authorization in securing these workflows, it is important to assess whether the current security specifications are adequate.

Currently, the authorization aspects outlined in TS 33.434 [2] can be limited to address the security requirements of AIMLE services. Therefore, this key issue aims to study whether enhancements to the authorization mechanisms specified in 3GPP TS 33.434 [2] are necessary to support AIMLE service security. The objective is to ensure trusted FL members participation, prevent unauthorized access of AIMLE operations.

### 4.1.2 Security threats

Unauthorized FL members participating in AIMLE services may gain access to data exchanged between AIMLE clients and servers.

Lack of robust authorization allows unreliable or unauthorized FL members to degrade the quality, efficiency, or availability of AIMLE operations.

### 4.1.3 Potential security requirements

The 3GPP system shall support authorization mechanisms for (FL members) utilising AIMLE services for various FL procedures.

## 4.2 Key Issue #2: Secure AIMLE ML Model Access

### 4.2.1 Key Issue details

TS 23.482 [3] describes AIMLE services which supports ML Model retrieval, ML model training, ML model management (model information storage and discovery) ML model update, and ML model selection aspects. AIMLE Services uses SEAL as the fundamental architecture and the authorization aspects of SEAL Security in TS 33.434 [2] which allows requested service specific authorization which can be limited and necessary controls can be in place for the different ML access and management work flow authorization for the overall AIMLE based ML access security.

### 4.2.2 Security threats

Unauthorized AIMLE client(s)/ VAL server using AIMLE services may gain access to ML model data leading to leakage of model.

Lack of robust authorization allows unauthorized AIMLE client(s) or VAL servers to degrade the quality, efficiency, or availability of AIMLE operations.

### 4.2.3 Potential security requirements

The 3GPP system shall support authorization to secure AIMLE service-based ML Model operations such as retrieval, training, update, selection, and management (i.e., ML model information storage and discovery).

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

### 4.X.1 Key Issue details

### 4.X.2 Security threats

### 4.X.3 Potential security requirements

# 5 Solutions

Editor’s Note: This clause contains the proposed solutions addressing the identified key issues.

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

### 5.Y.1 Introduction

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

### 5.Y.2 Solution details

### 5.Y.3 Evaluation

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

# 6 Conclusions

## 6.Z Key Issue #Z: <Key Issue Name>

Editor’s Note: This clause contains the agreed conclusions for Key Issue #Z.

Annex <A>: <Informative annex title for a Technical Report>

Annex <X>: Change history

|  |
| --- |
| Change history |
| Date | Meeting | TDoc | CR | Rev | Cat | Subject/Comment | New version |
| 2025-08 | SA3#123 | S3-252919 |  |  |  | AIMLE Service Security TR Skeleton | 0.0.0 |
| 2025-09 | SA3#123 | S3-253004 |  |  |  | Included Contributions: S3-253003, S3-253005 S3-253006 | 0.1.0 |