**3GPP TSG-SA3 Meeting #124 draft\_S3-253700-r1**

**Wuhan, China, 13 – 17 October 2025**

**Source: Huawei, HiSilicon**

**Title: Solution for KI #1**

**Document for: Approval**

**Agenda item: 5.2.3**

**Spec: TR 33.786**

**Version: 0.0.0**

**Work Item: FS\_AIMLE\_SEC**

**Comments**

This contribution proposes a solution on authorization of AIMLE clients acting as FL members for access to AIMLE service security.

\* \* \* First Change \* \* \* \*

# 2 References

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

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

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

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

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

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

[y] 3GPP TS 23.434: "Service Enabler Architecture Layer for Verticals (SEAL); Functionalarchitecture and information flows".

\* \* \* Next Change \* \* \* \*

## 5.Y Solution #Y: Authorization of AIMLE clients acting as FL members for access to AIMLE Service Security

### 5.Y.1 Introduction

This solution proposes the authorization of AIMLE clients in support of federated learning (FL). It ensures that only authorized clients (FL members) are selected and that secure token-based verification is performed using NEF. Tokens include only the minimum required claims such as ML model ID / Application Data Analytics Enablement (ADAE) analytics ID and ML model interoperability information to maintain security while ensuring interoperability.

### 5.Y.2 Solution details

#### 5.Y.2.1 The procedure for AIMLE clients’ authorization



Figure 5.Y.2-1 Authorization’s procedure of AIMLE clients acting as FL members

1. The VAL server sends a FL member grouping support request to the AIMLE server. The request includes the requestor ID, security credentials, and FL grouping criteria (e.g., grouping method, member selection criteria). The initial request is to create the FL member grouping support as described in Step 1 of clause 8.17.2 of TS 23.482 [x].

Editor ’s Note: The type, format, and validation procedure of the security credentials used in Step 1 are FFS.

2. Upon receiving the request, the AIMLE server validates whether the requestor is authorized to make it.

3. If authorized, the AIMLE server performs an FL member registration fetch with the ML repository based on the FL grouping criteria (see Step 3 of clause 8.17.2 in TS 23.482[x]).

4. The AIMLE server monitors AIMLE clients (FL members) to check whether they meet the selection criteria from step 1 as described in Step 4 of clause 8.13.2.2 of TS 23.482 [x]. AIMLE server interacts with NEF and/or SEAL services (including SEALDD) to set up monitoring. For location-based criteria, it uses SEAL-LMS (3GPP TS 23.434 [y] clauses 9.3.11/9.3.12) or 5GC services (e.g., NEF) to detect UEs entering or present in the target area.

5.a. Using monitoring results, the AIMLE server selects clients that meet the criteria and removes those that do not (e.g., due to location changes).

NOTE 1: The frequency at which monitoring results are provided is left to the implementation.

5.b. Each selected AIMLE client requests an access token from the AIMLE Server. The access token request sent to the AIMLE Server includes the following parameters: ML model ID / ADAE analytics ID and ML model interoperability information.

5.c. The AMILE server requests token from NEF on client’s behalf.

5.d. The NEF sends the generated access token to the AMILE server, which then returns the token to the client.

Editor ’s Note: The entity acting as the resource server for access token validation and protected resource access is FFS.

6.a. If AIMLE client obtains the access token, the AIMLE client sends a service request message to AIMLE server, requesting the AIMLE server to join FL group. The message contains the ML model ID / ADAE analytics ID and ML model interoperability information, and access token.

6.b. The AIMLE server triggers token verification with NEF. The NEF obtains the ML model ID / ADAE analytics ID and ML model interoperability information contained in the access token and verifies whether they match the corresponding values in step 5.d.

6.c. In case of successful access token verification, NEF respond to AIMLE server to retain the client.

Editor ’s Note: The issue and verification of token by NEF is FFS.

7. The AIMLE server performs the FL member grouping, notifies selected AIMLE clients of their group membership, collects acknowledgements, and returns a FL member grouping support response to the VAL server that includes success/failure status, grouping details, and an optional expiration time for the grouping.

### 5.Y.3 Evaluation

TBD

\* \* \* End of Changes \* \* \* \*