**3GPP TSG-SA3 Meeting #123 S3-253005**

**Goteborg, Sweden, 25 - 29 August 2025**

**Source: Huawei, HiSilicon, Lenovo**

**Title: New KI on Enhancing Authorization for AIMLE Service Security.**

**Document for: Approval**

**Agenda item: 6.1.1**

**Spec: None**

**Version: None**

**Work Item: Study on AIMLE Service Security**

**Comments**

The authorization mechanisms currently specified in TS 33.434 may not sufficiently address the unique security requirements of AIMLE services involving multiple AIMLE members. To ensure trusted members and prevent unauthorized or malicious access, SA3 should study whether enhancements to these authorization aspects are needed. This study should take into account the existing SEAL security mechanisms, as the AIMLE architecture is based on the SEAL framework and relevant SEAL security aspects may apply.

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

# 2 References

[x1] 3GPP TS 23.482: “Functional architecture and information flows for AIML Enablement Service”.

[x2] 3GPP TS 33.434: “Security aspects of Service Enabler Architecture Layer (SEAL) for verticals”.

\* \* \* Second Change \* \* \* \*

## Y.X. Key Issue #X: Authorization for AIMLE Service Security for FL members

### Y.X.1 Key issue details

3GPP TS 23.482[x1] 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 [x2] 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 [x2] are necessary to support AIMLE service security. The objective is to ensure trusted FL members participation, prevent unauthorized access of AIMLE operations.

### Y.X.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.

### Y.X.3 Potential security requirements

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

\* \* \* End of Change \* \* \* \*