**3GPP TSG-SA5 Meeting #157S5-245688**

Hyderabad , IN, 14 - 18 October 2024

**Source: Ericsson-LG CO, Intel**

**Title: Adding ML Authentication UseCase**

**Document for:Approval**

**Agenda Item: AIML\_MGT\_PH2**

# 1 Decision/action requested

***approval***

# 2 References

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

[2] 3GPP TS 28.105: Artificial Intelligence / Machine Learning (AI/ML) management".

[3] 3GPP TS 28.533: "Technical Specification Group Services and System Aspects".

# 3 Rationale

Secure authentication is crucial for maintaining the integrity and security of ML model training across all machine learning techniques, including centralized, distributed, and federated learning. It ensures that only authenticated entities contribute to the training process, preventing unauthorized access and maintaining data integrity.

This contribution proposes extending the existing MLTrainingFunction and MLTrainingReport IOCs to manage entity participation efficiently. By integrating authentication attributes, the solution enhances the security and reliability of the overall ML training process.

# 4 Detailed proposal

|  |
| --- |
| **Start of 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".

[2] 3GPP TS 28.105: Artificial Intelligence / Machine Learning (AI/ML) management".

[3] 3GPP TS 28.104: "Management and orchestration; Management Data Analytics".

[4] 3GPP TS 28.541: " Management and orchestration; 5G Network Resource Model (NRM); Stage 2 and stage 3".

[X] 3GPP TS 28.533: "Management and orchestration; Architecture framework".

|  |
| --- |
| **Next Change** |

## 5.1 ML model training

### **5.1.X ML Authentication**

#### **5.1.X.1 Description**

Authentication is a fundamental requirement for ensuring the integrity and security of the ML model training process. It is imperative that each participating entity, whether operating within a centralized, distributed, or federated learning environment, is authenticated is using a secure and reliable method. This practice serves to prevent unauthenticated access and guarantees that only verified enities will participate in the ML training process, thereby maintaining integrity, accuracy and reliability of the overall ML model.

As part of the training process, each participating entity should authenticate. The ML training function is responsible for validating these authentications to ensure that all entities participating on the ML Training process are verified.

The existing authentication mechanisms specified in **TS 28.533** [3]**, clause 4.9.1**, provide the necessary framework for ML authentication. These outline robust authentication services, including the use of certificates, tokens, or mutual authentication protocols, ensuring that only authenticated entities are permitted to contribute to the training process.

#### **5.1.X.2 Potential Requirements**

**REQ-ML\_AUTH-01:** The ML training MnS producer should support the capability to authenticate all participating entities involved in a training process.

#### **5.1.X.3 Possible Solution**

The authentication mechanisms specified in TS 28.533 [X], clause 4.9.1, provide the necessary framework for ML authentication in centralized, distributed, and federated learning environments. These mechanisms include secure methods such as certificates, tokens, and mutual authentication protocols, ensuring that only authorized entities participate in the ML model training process.

#### **5.1.X.4 Evaluation**

The solution in clause 5.1.X.3 is feasible, offering a simple and efficient approach by reusing the existing authentication mechanisms from TS 28.533. This approach minimizes complexity and requires no additional development in the normative specifications. Any more advanced solutions, if necessary, would require further investigation.

Bottom of Form

|  |
| --- |
| **End of Change** |