**3GPP TSG-SA3 Meeting #108Adhoc-e *draft\_S3-222500-r1***

**e-meeting, 10th – 14th October, 2022** Revision of S3-22xxxx

**Source: Huawei, HiSilicon**

**Title: New Solution based on reusing Existing Mechanism for AIML model storage and sharing**

**Document for: Approval**

**Agenda Item: 5.8**

# 1 Decision/action requested

***The contribution*** ***proposes a new solution to address KI#3 in TR 33.738.***

# 2 References

# 3 Rationale

This contribution propose a solution reusing the existing SBA security mechanisms to address authentication, authorization, and protection of AI/ML model storage and sharing. It is also proposed that security mechanisms for protection of AI/ML model in ADRF are left to implementation

# 4 Detailed proposal

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of 1st 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 23.501: "System Architecture for the 5G System; Stage 2".

[3] 3GPP TS 23.502: "Procedures for the 5G system, Stage 2".

[4] 3GPP TS 23.503: "Policy and Charging Control Framework for the 5G System".

[5] 3GPP TS 23.288: "Architecture enhancements for 5G System (5GS) to support network data analytics services".

[6] 3GPP TR 23.700-81: " Study of Enablers for Network Automation for 5G System (5GS); Phase 3".

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

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of 1st Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of 2nd Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

## 6.X Solution #X: Reusing Existing Mechanism for AI/ML model storage and sharing

### 6.X.1 Introduction

This solution addresses key issue#3 on security for AI/ML model storage and sharing. For AI/ML model sharing, it is proposed to reuse SBA security mechanisms for authentication, authorization, integrity, confidentiality and replay protection. For AI/ML model storage, since it is not standard issue, it is proposed that security mechanisms for protection of AI/ML model in ADRF are left to implementation.

### 6.X.2 Solution details

Any AI/ML model transferred between core network functions is protected by reusing the existing SBA security mechanisms. According to TS 33.501 [xx], clause 13.1.0, TLS is mandatory to support. When TLS is used, any exchange of information including AI/ML models between NFs is integrity, confidentiality and replay protected.

Any NF (e.g. NWDAF) that is directly or indirectly requesting AI/ML model from ADRF is authorized by reusing the existing SBA security mechanisms. According to TS 33.501 [xx], clause 13.3 or 13.4, both static authorization and OAuth2.0 token based authorization are two candidate mechanisms that can be reused.

### Security mechanisms for protection of AI/ML model in ADRF are left to implementation, which is similar with UDM requirement for long-term key storage as depicted in clause 5.8.1 in TS 33.501 [xx].6.X.3 Evaluation

TBA

Editor’s Note: Clarification on how ML models leak is prevented between entity producing the ML model (e.g., MTLF) and NFc is ffs, if the ADRF itself cannot be considered a fully trusted entity.

Editor’s Note: Whether or not model retrieval from the ADRF uses SBA is pending conclusion in SA2.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of 2nd Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*