**3GPP TSG-SA3 Meeting #110Ad-Hoc-e *draft\_S3-231746-r5***

**Electronic meeting, Online, 17 - 21 April 2023** (revision of S3-yyxxxx)

**Source: Ericsson, Nokia, Intel**

**Title: Resolve first EN to conclusion to KI#3 "Security for AI/ML model storage and sharing"**

**Document for: Approval**

**Agenda Item: 5.8**

# 1 Decision/action requested

***Approve the pCR to TR 33.738 [1] below.***

# 2 References

[1] 3GPP TR 33.738 1.0.0 "Study on security aspects of enablers for Network Automation for 5G - phase 3"

[2] 3GPP TS 23.288 v18.1.0 "Architecture enhancements for 5G System (5GS) to support network data analytics services"

# 3 Rationale

This contribution proposes a resolution of this Editor's Note in the conclusion to KI#3 "Security for AI/ML model storage and sharing":

Editor’s Note: Whether vendor id is used for authorization of NF service consumer is FFS and needs to align with SA2.

It is already concluded that the NF Service Producer indicates its interoperability indicator during registration at the NRF. According to TS 23.288, clause 5.2:

"The ML Model Interoperability indicator comprises a list of NWDAF providers (vendors) that are allowed to retrieve ML models from this NWDAF containing MTLF. It also indicates that the NWDAF containing MTLF supports the interoperable ML models requested by the NWDAFs from the vendors in the list."

For example, say an NWDAF 1 containing both MTLF and AnLF registers an interoperability indicator that contains vendor A and vendor B, and NWDAF 2 containing MTLF registers an interoperability indicator that contains vendor B and vendor C. If NWDAF 1 requests from the NRF an access token for access to models from NWDAF 2, the NRF does not have enough information to grant the access token to NWDAF 1, since the NRF does not know whether NWDAF 1 is from vendor A or vendor B. If, additionally, NWDAF 1 registers as OAuth 2.0 client with Vendor ID vendor B, the NRF has enough information and can grant the access token to NWDAF 1.

Therefore, the Vendor ID is indeed necessary for the authorization of NF Service Consumers.

# 4 Detailed proposal

\*\*\* BEGIN CHANGES \*\*\*

7.3 Conclusion on Key Issue #3 "Security for AI/ML model storage and sharing"

The conclusions for KI#3 are:

- Authorization of the model retrieval at the NRF uses OAuth 2.0 token-based authorization. The NRF uses information provided by the NF service producer (NWDAF MTLF) and information provided by the NF service consumer (e.g. NWDAF AnLF).

- The NF service producer (NWDAF MTLF) needs to be registered in the NRF, indicating the NF service producer information (including interoperability indicator per Analytics ID) that is used by the NRF to decide whether the consumer is authorized. The NF service consumer (e.g. NWDAF AnLF) needs to be registered in the NRF as OAuth 2.0 client, indicating the NF service consumer information(including Vendor ID) that is used by the NRF to decide whether the consumer is authorized.

- The NF service consumer (e.g AnLF) includes the desired Analytics ID(s) in the access token request. The NRF checks whether the NF service consumer is authorized to retrieve models for this Analytics ID(s). If the NF consumer is authorized, the NRF issues an access token with the Analytics(s) included in the access token.

Editor's Note : The requirement for the AI/ML model to be stored in encrypted format and corresponding key management aspects are ffs.

- As per the request of Analytics Id by the NFc, the MTLF performs authorization of the corresponding model retrieval per selected model.

NOTE: the model delivery procedure is to be defined by 3GPP SA2.

- The granularity of the authorization at AI/ML model level is performed at MtLF.

- ADRF verifies that the requested AI/ML model can be retrieved by the NF consumer(s) (MTLF or AnLF), based on the decision by the MtLF.

\*\*\* END CHANGES \*\*\*