**3GPP TSG-SA3 Meeting #102Bis-e *S3-211039***

**e-meeting, 1 – 5 March 2021** *Revision of S3-21XXXX*

**Source: Nokia, Nokia Shanghai Bell**

**Title: KI on Ensuring restrictive transfer of ML models between authorized NWDAF Instances**

**Document for: Approval**

**Agenda Item: 5.16**

# 1 Decision/action requested

***New KI to eNA study TR33.866 on ensuring*** ***restrictive transfer of ML models between authorized NWDAF Instances***

# 2 References

[1] 3GPP TR 23.700-91: “Study on enablers for network automation for the 5G System (5GS); Phase 2”

# 3 Rationale

SA2 agreed that NWDAF instances can discover other NWDAF instances providing ML models via NRF. In the current release sharing of ML models or model meta data is limited to a single vendor environment. Adequate security mechanisms are needed to ensure that the models are indeed only transferred between authorized NWDAF instances.

# 4 Detailed proposal

\*\*\*\*\*\*\*\*\*\* START OF CHANGES

### 5.3.X Key Issue #3.X: Ensuring restrictive transfer of ML models between authorized NWDAF instances

#### 5.3.X.1 Key issue details

In 3GPP TR 23.700-91 [X], Key Issue 19 describes trained model sharing between multiple NWDAF Instances. As quoted below, the model sharing will be limited to single vendor environment:

*"3GPP standardized sharing of models across different vendor environments is not deemed feasible in this release of the specifications. Sharing of models or model meta data is limited to single vendor environments."*

 As described in 3GPP TR 23.700-91 [X], NWDAF instances can discover other NWDAF instances providing ML models via NRF. Currently no mechanism exists, which can ensure that ML models are only shared between the NWDAF instances of the same vendor.

Since machine learning models are trained using proprietary algorithms, and sometimes are also trained using sensitive data, securing them and ensuring restricted and safe transfer is paramount. Therefore, this key issue will study how to ensure that trained model sharing is only allowed at the same trust domain, e.g. by the same vendor.

#### 5.3.X.2 Security Threats

If ML models are shared with a NF, which is not part of the same trust domain, it can be reverse engineered to expose proprietary and sensitive implementation specific information.

#### 5.3.X.3 Potential security requirements

Only authorized NWDAF instances should be allowed to consume ML models from other NWDAF instances.

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