**3GPP TSG-SA3 Meeting #108e-AdHoc *draft\_S3-222788-r1***

e-meeting, 10 - 14 October 2022

**Title:** **[DRAFT] Reply LS on how ML model integrity, confidentiality and availability is supported between NWDAFs from different vendors**

**Response to:** **LS (S2-2207156) on how ML model integrity, confidentiality and availability is supported between NWDAFs from different vendors**

**Release:** **Rel-18**

**Work Item:** **FS\_eNA\_SEC\_Ph3**

**Source:** **Ericsson, to be SA3**

**To:** **SA2**

**Cc:** -

**Contact person:** **Ferhat Karakoc**

 **ferhat dot karakoc at ericsson dot com**

**Send any reply LS to:** **3GPP Liaisons Coordinator, mailto:3GPPLiaison@etsi.org**

**Attachments:** None

1 Overall description

SA3 would like to thank SA2 for the LS on how ML model integrity, confidentiality and availability is supported between NWDAFs from different vendors (S2-2207156) and would like to reply to the following question:

***Question to SA3:*** *How is ML model integrity, confidentiality and availability supported when NWDAF containing MTLF and NWDAF containing AnLF are from different vendors?*

Regarding the ML model integrity and confidentiality in the context of ML model sharing between NWDAFs from different vendors, SA3 has a related key issue which is being studied in TR 33.738 and SA3 will inform SA2 when the conclusions are agreed on. Regarding the ML model availability, SA3 thinks that this aspect should be under SA2’s remit.

For studying the necessity on the E2E protection of ML models, SA3 need the following question answered:

Is there any possibility that ADRF or the repository where stores ML models located outside the operator’s domain ?

2 Actions

**To SA2**

**ACTION:** 3GPP SA3 kindly asks SA2 to take the above into account and answer the question above.

3 Dates of next TSG SA WG 3 meetings

SA3#109 14 - 18 November 2022 Toulouse (France)

SA3#110e 16 - 20 January 2023 Online (electronic meeting)