**3GPP TSG-SA3 Meeting #108-e *S3-222046-r1***

**e-meeting, 22th August – 26th August 2022**

**Source: Intel**

**Title: Privacy-Preserving Machine Learning**

**Document for: Approval**

**Agenda Item: 5.14**

# 1 Decision/action requested

***This pCR adds a key issue to TR 33.877.***

# 2 References

[1] 3GPP TR 37.817: "Study on enhancement for data collection for NR and ENDC".

# 3 Rationale

Pcr Adds a key issue related UE sensitive information exposure

# 4 Detailed proposal

SA3 is kindly requested to agree on the pCR below to TR 33.877

\*\*\*\*\*Start of Changes\*\*\*\*\*

5.X Key Issue #X: Privacy-Preserving Machine Learning

5.X.1 Key issue details

In 3GPP TR 33.817 [1], a high-level architectural principle states, "User data privacy and anonymization should be respected during AI/ML operation.”.. OAM and /or NG-RAN node may train a model or perform inference using the the UE related information interpreted by gNB (e.g., UE location information and UE trajectory prediction), and the information obtained from neighbour gNB (e.g., UE mobility history information). Such information may include UE’s sensitive information such as user identifier and location or may expose the UE..

5.X.2 Security threats

Without privacy protection mechanisms, the privacy information of UE (e.g., location information of UE) may increase exposure to NG-RAN nodes.

5.X.3 Potential security requirements

The 5G System shall support privacy protection for the use cases of Network Energy Saving, Load Balancing and Mobility Optimization of the RAN AI/ML framework.

.

\*\*\*\*\*End of Changes\*\*\*\*\*