**3GPP TSG-SA3 Meeting #102e *S3-210189***

**e-meeting, 18 – 29 January 2021**

**Source: CATT**

**Title: Add new key issue in TR 33.866**

**Document for: Approval**

**Agenda Item: 5.16**

# 1 Decision/action requested

***It is proposed to add one new key issue in TR 33.866. SA3 is kindly requested to approve this contribution.***

# 2 References

[1] 3GPP TR 33.866, v0.2.0

# 3 Rationale

This pCR proposes to add one new key issue for the security of eNA.

# 4 Detailed proposal

\*\*\*\*\*\* FIRST OF CHANGE \*\*\*\*\*\*\*\*\*

5.1.X Key Issue #1.X The data protection of Data Management Framework related interfcace

5.1.X.1 Key issue details

As specified in TS 23.900-91[1], data management function is decoupled from analysis functions for the NWDAF in Rel-17. The NWDAF is decomposed by moving Data Collection, including the task of identifying the Data Source, to the Data Management Framework. New NFs (e.g. DCCF, DRF) are specified. If the DCCF and DRF are implemented as standalone NFs, the new interfaces are introduced.

In Rel-17, Data Collection Coordination Functionality (DCCF) is used to coordinate collection of data from one or more NF(s) based on data collection requests from one or more Consumer NF(s). The NWDAF requests Data from the Data Management Framework. And if the data is not collected, the Data Management Framework will request the data from a data source. In other words, the Data Source will independently send data back to the Data Management Framework that sent the request for the NWDAF(s).

DRF functionality is used to store data as specified in TS 23.900-91[1].

As concluded in clause 8 in TR 23.900-91[1], Data Collection Coordination Functionality (DCCF) and Data Repository Functionality (DRF) and the related interfaces (e.g. data collection, data request) are to be standardized.

5.1.X.2 Security threats

An attacker may eavesdrop or manipulate or replay the communication or initiate the MITM attacks on the interface without confidentiality, integrity and replay protection,

5.1.X.3 Potential security requirements

Confidentiality protection, integrity protection and replay-protection shall be supported on the new interfaces.

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