**3GPP TSG-SA3 Meeting #100bis-e *S3-202530-r1***

**e-meeting, 12-16 October 2020** Merger of S3-202420 and S3-202530

**Source: Ericsson, Nokia, Nokia Shanghai Bell**

**Title: A new key issue on security of data collection from UE**

**Document for: Approval**

**Agenda Item: 2.16**

# 1 Decision/action requested

***Approve this contribution to add a new key issue in the eNA study TR33.866***

# 2 References

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

# 3 Rationale

In [1], Key Issue #8 "UE data as an input for analytics generation" addresses whether and how to enhance the 5GS to support collection and utilisation of data provided by the UE in NWDAF in order to provide input information to generate analytics information (to be consumed by other NFs). This key issue addresses the security of data collection from the UE.

# 4 Detailed proposal

\*\*\* BEGINNING OF 1st CHANGES \*\*\*

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

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

\*\*\* END OF 1st CHANGES \*\*\*

\*\*\* BEGINNING OF 2nd CHANGES\*\*\*

## 4.X Key Issue #X: Security of data collection from UE

### 4.X.1 Key issue details

In [xx], Key Issue #8 "UE data as an input for analytics generation" addresses whether and how to enhance the 5GS to support collection and utilisation of data provided by the UE in NWDAF in order to provide input information to generate analytics information (to be consumed by other NFs). This key issue addresses the security of data collection from the UE.

### 4.X.2 Threats

If the application in UE is not authenticated by the network, then an unauthorized entity can send data on behalf of a UE, which may cause wrong analytic results.

If an unauthenticated UE is sending the data , it may send erroneous data to NF/NWDAF, it can compromise the efficiency, performance and output of analytics algorithms implemented in the analytics functions.

In case of the network is not authenticated by the application in UE, the application in UE may send UE data to an unauthorized entity, which may lead to leakage of sensitive data of the UE.

If the NF/NWDAF which is receiving UE data is not properly authenticated and authorized, the sender may transfer the UE data to an unauthorized NF or analytics function.

If the communication between the application in UE and network is not confidentiality protected, then sensitive information about UEs may be leaked to unauthorized entities.

If the integrity of the data collected from UE is not protected, the analytics may not be accurate.

Replay attacks may lead to usage of same UE data more than once, and therefore, it may cause wrong analytic results.

### 4.X.3 Potential Security requirements

The transfer of UE data shall be confidentiality, integrity and replay protected.

The application in UE and network shall be mutually authenticated.

\*\*\* END OF 2nd CHANGES \*\*\*