**3GPP TSG-SA3 Meeting #102-e *draft\_S3-210107-r1***

**e-meeting, 18 – 29 January 2021** *Revision of S3-210107*

**Source: Nokia, Nokia Shanghai Bell**

**Title: KI on protection of data in transit**

**Document for: Approval**

**Agenda Item: 5.16**

# 1 Decision/action requested

***New KI to eNA study TR33.866 on protection of data in transit.***

# 2 References

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

# 3 Rationale

UE data is input for analytics generation by NWDAF to be consumed by other NFs. This key issue addresses the security of UE related data transferred between core functions.

# 4 Detailed proposal

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

### 5.3.X Key Issue #3.X: Protection of UE data in transit

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

The UE is providing the core network functions with data, which are reported to or requested by analytics functions. The transfer of any data between core network functions needs to be protected.

According to TS 23.288 [y] the NWDAF collects data from various data sources and provides Analytics Output to different NWDAF data consumers. In addition, according to the solutions for KI#2 "Multiple NWDAF Instances" proposed in TR 23.700-91 [x] the analytics data or the analytics output can be transferred from one NWDAF instance to another NWDAF instance.

Data in transit needs to be protected while in transfer between NWDAFs, NF to NWDAFs and NWDAF to another entity, e.g. DCCF.

This key issue addresses security for data in transit involving an analytics function.

#### 5.3.X.2 Security Threats

If data is transferred between NFs or different NWDAF Instances, a MitM (for instance a malicious SCP) can compromise data by eavesdropping or modification.

A rogue NWDAF Instance can send wrong or modified data to another NWDAF instance.

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

Data transferred between core network functions shall be integrity, confidentiality and replay protected.

\*\*\*\*\*\*\*\*\* next change

### 5.3.X Key Issue #3.X: Assuring genuine source and recipient for data in transit

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

The UE is providing the core network functions with data, which are reported to or requested by analytics functions.

According to TS 23.288 [y] the NWDAF collects data from various data sources and provides Analytics Output to different NWDAF data consumers. In addition, according to the solutions for KI#2 "Multiple NWDAF Instances" proposed in TR 23.700-91 [x] the analytics data or the analytics output can be transferred from one NWDAF instance to another NWDAF instance.

Therefore, transfer of any data between NFs and NWDAF and between different NWDAF instances needs to be authorized to ensure that data comes from a genuine source as well as that the target NF is genuine and authorized to receive the data.

#### 5.3.X.2 Security Threats

A rogue NWDAF Instance can send data to another entity without checking that the receiver is genuine and authorized to receive the data.

A rogue target NWDAF Instance is able to receive data unauthorized.

An NF can consume analytics data without being authorized.

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

Only authorized NFs shall be allowed to consume UE data from the analytics function.

The target NWDAF Instance shall be authorized to receive data from another NWDAF.

It shall be ensured that data is coming from a genuine NWDAF Instance ID which has been collecting this data.

The source NWDAF Instance shall check if the receiver is genuine and authorized to receive the data.

NOTE: It is expected that these requirements can be fulfilled by existing 5GS security mechanisms.

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