**3GPP TSG-SA3 Meeting #101-e *draft\_S3-210112-r1***

**e-meeting, 18 – 29 January 2021** *Revision of S3-210112*

**Source: Nokia, Nokia Shanghai Bell**

**Title: KI on UE data collection protection**

**Document for: Approval**

**Agenda Item: 5.16**

# 1 Decision/action requested

***New KI to eNA study TR33.866 on UE data collection protection at NF/NWDAF***

# 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.

-r1 merging in S3-210113 (threats and requirements)

# 4 Detailed proposal

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

### 5.1.X Key Issue #1.X: UE data collection protection at NF/NWDAF

#### 5.1.X.1 Key issue details

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.

UEs register to 5GS and request services, e.g. the initial registration request to AMF. For fulfilling the service, but also for analytics purposes, 5GS NFs will collect data about the UE being served, e.g. AMF needs to maintain a mapping between SUPI and 5G-GUTI and for accounting the time window for the service used. UE related data, processed by one NF, may also need to be transferred to another NF to fulfil a service request or for analytics purposes. UE can also provide privacy sensitive data such as positioning information, user profiling info, etc to NFs, which may be transferred to NWDAF.

This KI determines the threats and requirements for protection of UE data collected by core NFs.

#### 5.1.X.2 Security threats

If the communication between 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 application is not protected, the analytics may not be accurate.

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

A NF can collect from UE applications privacy sensitive information about UEs such as location information, environment information, user profile information, which UE is not informed about. This is compromising the UE's privacy. If NF collects data from UE application without taking into consideration the user consent, the UE is not in control of its own data and loses its right of data protection.

Data collected from UE applications and stored in a NF or transferred between different NFs may be altered by a malicious entity. The attacker may provide false or modified information to other NFs or an analytics function such as NWDAF. For instance, the malicious entity can modify the UE information statistics or logs sent to the NWDAF.

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

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

#### 5.1.X.3 Potential Security requirements

UE and network shall mutually authenticate each other.

The communication between UE and network shall be confidentiality protected.

The data collected from UE application shall be integrity protected.

Data transferred from UE to NFs and from NFs to the analytics function shall be protected against replay attacks.

Authorization of NFs and analytics functions to receive, send, or transfer data shall be guaranteed.

It shall be possible to process user consent depending on the regulatory and regional demands.

Note: Any solution related to this requirement is further handled in the user consent study FS\_UC3S.

It shall be possible to respect user privacy depending on the regulatory and regional demands.

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