**3GPP TSG-SA3 Meeting #101-e *S3-210114***

**e-meeting, 18 – 29 January 2021** *Revision of S3-21XXXX*

**Source: Nokia, Nokia Shanghai Bell**

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

**Document for: Approval**

**Agenda Item: 5.16**

# 1 Decision/action requested

***Solution on UE data collection protection at NF/NWDAF to 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).

Key issue 1.X proposes in an accompanying contribution that 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.

The transport of data between UE and NF/NWDAF needs therefore protection, which is expected to simply re-use the current NAS and AS security mechanisms as well as SBA as proposed in the following as solution.

# 4 Detailed proposal

It is requested to include the following solution related to key issue on UE data collection protection at NF/NWDAF related to key issue group #1.

\*\*\*\*\*\*\*\*\*\* START OF 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*.

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

[2] 3GPP TS 33.867: "Study on user consent for 3GPP services".

[3] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[4] 3GPP TS 23.288: "Architecture enhancements for 5G System (5GS) to support network data analytics services ".

[5] 3GPP TS 23.501: "System Architecture for the 5G System; Stage 2".

[6] Draft NISTIR 8269: "A Taxonomy and Terminology of Adversarial Machine Learning; <https://doi.org/10.6028/NIST.IR.8269-draft>".

[7] ETSI SAI: "AI Threat Ontology: <https://docbox.etsi.org/ISG/SAI/70-DRAFT/001/SAI-001v008.docx>".

[8] 3GPP TS 33.501: "Security architecture and procedures for 5G system".

\*\*\*\*\*\*\*\*\*\* NEXT CHANGE

## 6.0 Mapping of solutions to key issues

Table 6.0-1: Mapping of solutions to key issues

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Solutions | Key Issues | | | | | | | | |
| 1 Key issues related to securing the data provided to any type of analytics function | | | 2 Key issues related to detection of cyber-attacks and anomaly events by analytics function | | | 3 Key issues related to data transfer protection | | |
|  | 1.1 | 1.2 | 1.X | 2.1 | 2.2 | 2.Y | 3.1 | 3.Z |  |
| #Y: UE data collection protection |  |  | X |  |  |  |  |  |  |
| #X: <Solution name> |  |  |  |  |  |  |  |  |  |

## 

\*\*\*\*\*\*\*\*\*\* NEXT CHANGE

## 6.Y Solution #Y: UE data collection protection

### 6.Y.1 Introduction

This solution addresses KI#1.X on UE data collection protection at NF/NWDAF

### 6.Y.2 Solution details

For enhancing 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) the communication between UE and NF/NWDAF needs to be secured.

In line with 5GS generic security requirements it is therefore proposed that the transfer of data between UE and NF/NWDAF related to UE data collection re-uses existing 5GS security mechanisms.

For UE data collection by NFs and NWDAF, the current NAS and AS security mechanisms for authentication, confidentiality, integrity and replay protection as described in 3GPP TS 33.501 are used.

NOTE: Whether user consent is necessary is subject of the user consent study FS\_UC3S.

For transfer of UE data to NF/NWDAF privacy requirements could apply.

### 6.Y.3 Evaluation

TBD

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