**3GPP TSG-SA3 Meeting #101e S3-203125**

**e-meeting, 9 – 20 November 2020 Revision of S3-20xxxx**

**Source: China Mobile**

**Title: Proposal to add introduction and NWDAF-specific security functional requirements**

**Document for: Approval**

**Agenda Item: 4.18**

# 1 Decision/action requested

***It proposes to add introduction and NWDAF specific security functional requirements and related test cases in TS33.521.***

# 2 References

[1] TS 33.521, 5G Security Assurance Specification (SCAS); Network Data Analytics Function (NWDAF)

[2] TS 33.117, Catalogue of general security assurance requirements

# 3 Rationale

This contribution propose to add introduction description and new requirement for NWDAF.

# 4 Detailed proposal

pCR

\*\*\* BEGINNING 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 21.905: "Vocabulary for 3GPP Specifications".

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

[y] 3GPP TS 33.117: " Catalogue of general security assurance requirements "

[z] 3GPP TR 33.926: " Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes"

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

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

4 NWDAF-specific security requirements and related test cases

4.1 Introduction

NWDAF specific security requirements include both requirements derived from NWDAF specific security functional requirements in relevant specifications as well as security requirements introduced in the present document derived from the threats specific to NWDAF as described in TR 33.926 [z].

4.2 NWDAF-specific security functional requirements and related test cases

Editor’s Note: This clause will document NWDAF-specific security functional requirements and related test cases. The templates of the security requirements and test case are same with the used templates in TS 33.116.

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

### 4.2.Y Technical baseline

#### 4.2.Y.1 General

The present clause provides baseline technical requirements.

#### 4.2.Y.2 Protecting data and information

4.2.Y.2.1 Protecting data and information – general

There are no NWDAF-specific additions to clause 4.2.3.2.1 of TS 33.117 [y].

4.2.Y.2.2 Protecting data and information – Confidential System Internal Data

There are no NWDAF-specific additions to clause 4.2.3.2.2 of TS 33.117 [y].

4.2.Y.2.3 Protecting data and information in storage

There are no NWDAF-specific additions to clause 4.2.3.2.3 of TS 33.117 [y].

4.2.Y.2.4 Protecting data and information in storage

There are no NWDAF-specific additions to clause 4.2.3.2.4 of TS 33.117 [y].

4.2.Y.2.5 Protecting data and information in storage

There are no NWDAF-specific additions to clause 4.2.3.2.5 of TS 33.117 [y].

##### 4.2.Y.2.6 Protecting data and information – Data masking on integration analysis

Requirement Name: Data masking on integration analysis about personal data

Requirement Reference:TBA.

Requirement Description: NWDAF can collect data from UE, NF, OAM, etc. used for analytics. Personal data of the UE’s user are involved also. When NWDAF uses such personal data in analytics with other information together, such data correlation operation could bind more personal information with the user’s identity. Thus, privacy sensitive information about that specific user could be revealed to the person who is allowed to operate data correlation for analytics but not allowed to know the privacy information as the result of data correlation. Therefore, applicable measures (e.g. data masking) shall be applied to mitigate such privacy violation risk.

*Threat References*: TR33.926[z], clause 5.3.6.7, Personal Identification Information Violation

**Test Name**: TC\_DATA\_MASKING

**Purpose**:

Verify that no privacy information of operators’ users is revealed to the party who is not allowed to have.

**Pre-Condition**:

TBD.

**Execution Steps**

TBD

**Expected Results**:

TBD

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