ETSI TS 133 521 V19.0.0 (2025-10)

TECHNICAL SPECIFICATION

5G;
5G Security Assurance Specification (SCAS);
Network Data Analytics Function (NWDAF)
(3GPP TS 33.521 version 19.0.0 Release 19)

Reference
RTS/TSGS-0333521vj00

Keywords
5G,SECURITY

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI IPR online database.

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Legal Notice

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities. These shall be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between 3GPP and ETSI identities can be found at 3GPP to ETSI numbering cross-referencing.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Contents

Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

In the present document, modal verbs have the following meanings:

shall indicates a mandatory requirement to do something

shall not indicates an interdiction (prohibition) to do something

The constructions "shall" and "shall not" are confined to the context of normative provisions, and do not appear in Technical Reports.

The constructions "must" and "must not" are not used as substitutes for "shall" and "shall not". Their use is avoided insofar as possible, and they are not used in a normative context except in a direct citation from an external, referenced, non-3GPP document, or so as to maintain continuity of style when extending or modifying the provisions of such a referenced document.

should indicates a recommendation to do something

should not indicates a recommendation not to do something

may indicates permission to do something

need not indicates permission not to do something

The construction "may not" is ambiguous and is not used in normative elements. The unambiguous constructions "might not" or "shall not" are used instead, depending upon the meaning intended.

can indicates that something is possible

cannot indicates that something is impossible

The constructions "can" and "cannot" are not substitutes for "may" and "need not".

will indicates that something is certain or expected to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

will not indicates that something is certain or expected not to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

might indicates a likelihood that something will happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

might not indicates a likelihood that something will not happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

In addition:

is (or any other verb in the indicative mood) indicates a statement of fact

is not (or any other negative verb in the indicative mood) indicates a statement of fact

The constructions "is" and "is not" do not indicate requirements.

1 Scope

The present document contains requirements and test cases that are specific to the NWDAF network product class. It refers to the Catalogue of General Security Assurance Requirements and formulates specific adaptions of the requirements and test cases, as well as specifying requirements and test cases unique to the NWDAF network product class.

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".

[2] 3GPP TS 23.288: "Architecture enhancements for 5G System (5GS) to support network data analytics services".

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

[4] 3GPP TR 33.926: "Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes".

[5] 3GPP TS 23.501: "System Architecture for 5G System (5GS)".

3 Definitions of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in TR 21.905 [1].

3.2 Symbols

Void

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in TR 21.905 [1].

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 [4].

4.2 NWDAF-specific security functional requirements and related test cases

4.2.1 Technical baseline

4.2.1.1 General

The present clause provides baseline technical requirements.

4.2.1.2 Protecting data and information

4.2.1.2.1 Protecting data and information – general

There are no NWDAF-specific additions to clause 4.2.3.2.1 of TS 33.117 [3].

4.2.1.2.2 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 [3].

4.2.1.2.3 Protecting data and information in storage

There are no NWDAF-specific additions to clause 4.2.3.2.3 of TS 33.117 [3].

4.2.1.2.4 Protecting data and information in transfer

There are no NWDAF-specific additions to clause 4.2.3.2.4 of TS 33.117 [3].

4.2.1.2.5 Logging access to personal data

There are no NWDAF-specific additions to clause 4.2.3.2.5 of TS 33.117 [3].

4.2.1.2.6 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 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: TR 33.926 [4], 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:

The vendor shall provide the documentation describing how to create an account for accessing the analytics results.

Privacy information list (should be specified based on local policy, regulation and others).

Execution Steps:

1. Review the documentation provided by the vendor describing how to create the account for accessing the analytics results provided by the NWDAF.
2. The tester creates the account, and retrieves the analytics results from the NWDAF using the account.

Expected Results:

The tester can create the account, and the account does not reveal subscriber permanent identifier.

Expected format of evidence:

Evidence suitable for the interface, e.g. screenshot containing the results.

4.2.2 Void

4.3 NWDAF-specific adaptations of hardening requirements and related test cases

4.3.1 Introduction

The present clause contains NWDAF-specific adaptations of hardening requirements and related test cases.

4.3.2 Technical baseline

There are no NWDAF-specific additions to clause 4.3.2 of TS 33.117 [3].

4.3.3 Operating systems

There are no NWDAF-specific additions to clause 4.3.3 of TS 33.117 [3].

4.3.4 Web servers

There are no NWDAF-specific additions to clause 4.3.4 of TS 33.117 [3].

4.3.5 Network devices

There are no NWDAF-specific additions to clause 4.3.5 of TS 33.117 [3].

4.3.6 Network functions in service-based architecture

There are no NWDAF-specific additions to clause 4.3.6 in TS 33.117 [3].

4.4 NWDAF-specific adaptations of basic vulnerability testing requirements and related test cases

4.4.1 Introduction

There are no NWDAF specific addtions to clause 4.4.1 of TS 33.117 [3].

4.4.2 Port scanning

There are no NWDAF specific addtions to clause 4.4.2 of TS 33.117 [3].

4.4.3 Vulnerability scanning

There are no NWDAF specific addtions to clause 4.4.3 of TS 33.117 [3].

4.4.4 Robustness and fuzz testing

The test cases under clause 4.4.4 of TS 33.117 [3] are applicable to NWDAF.

The interface defined for the NWDAF are in 4.2.3 of TS 23.501 [5].

According to clause 4.4.4 of TS 33.117 [3], the transport protocols available on the interfaces providing IP-based protocols need to be robustness tested. Following TCP/IP layer model and considering all the protocols over transport layer, for NWDAF, the following interface and protocols are in the scope of the testing:

- For Nnwdaf: the TCP, HTTP2 and JSON protocols.

NOTE: There could be other interfaces and/or protocols requiring testing under clause 4.4.4 of TS 33.117 [3]

Annex A (informative): Change history

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
2021-06	SA#92e	SP-210427				Presented for information and approval	1.0.0
2021-06	SA#92e					EditHelp review and upgrade to change control version	17.0.0
2021-09	SA#93e	SP-210898	0002	1	F	Clarification on Data Masking on Integration Analysis	17.1.0
2022-06	SA#96	SP-220547	0003	-	F	Delete Use Case on Finding the right NF instance are serving the UE	17.2.0
2023-06	SA#96	SP-230677	0004	1	B	Robustness interfaces and protocols defined for NWDAF	18.0.0
2025-10	-	-	-	-	-	Update to Rel-19 version (MCC)	**19.0.0**

History

Document history		
V19.0.0	October 2025	Publication