

3GPP TS 33.521 V19.0.0 (2025-10)

Technical Specification

3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 5G Security Assurance Specification (SCAS); Network Data Analytics Function (NWDAF) (Release 19)



The present document has been developed within the 3rd Generation Partnership Project (3GPP™) and may be further elaborated for the purposes of 3GPP. The present document has not been subject to any approval process by the 3GPP Organizational Partners and shall not be implemented. This Specification is provided for future development work within 3GPP only. The Organizational Partners accept no liability for any use of this Specification. Specifications and Reports for implementation of the 3GPP™ system should be obtained via the 3GPP Organizational Partners' Publications Offices.

3GPP

Postal address

3GPP support office address

650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet

<http://www.3gpp.org>

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© 2025, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).
All rights reserved.

UMTS™ is a Trade Mark of ETSI registered for the benefit of its members
3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners
LTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners
GSM® and the GSM logo are registered and owned by the GSM Association

Contents

Foreword.....	4
1 Scope.....	6
2 References.....	6
3 Definitions of terms, symbols and abbreviations.....	6
3.1 Terms.....	6
3.2 Symbols.....	6
3.3 Abbreviations.....	6
4 NWDAF-specific security requirements and related test cases.....	7
4.1 Introduction.....	7
4.2 NWDAF-specific security functional requirements and related test cases.....	7
4.2.1 Technical baseline.....	7
4.2.1.1 General.....	7
4.2.1.2 Protecting data and information.....	7
4.2.1.2.1 Protecting data and information – general.....	7
4.2.1.2.2 Protecting data and information – Confidential System Internal Data.....	7
4.2.1.2.3 Protecting data and information in storage.....	7
4.2.1.2.4 Protecting data and information in transfer.....	7
4.2.1.2.5 Logging access to personal data.....	7
4.2.1.2.6 Protecting data and information – Data masking on integration analysis.....	7
4.2.2 Void.....	8
4.3 NWDAF-specific adaptations of hardening requirements and related test cases.....	8
4.3.1 Introduction.....	8
4.3.2 Technical baseline.....	8
4.3.3 Operating systems.....	8
4.3.4 Web servers.....	8
4.3.5 Network devices.....	8
4.3.6 Network functions in service-based architecture.....	8
4.4 NWDAF-specific adaptations of basic vulnerability testing requirements and related test cases.....	9
4.4.1 Introduction.....	9
4.4.2 Port scanning.....	9
4.4.3 Vulnerability scanning.....	9
4.4.4 Robustness and fuzz testing.....	9
Annex A (informative): Change history.....	9

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 adaptations 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 additions to clause 4.4.1 of TS 33.117 [3].

4.4.2 Port scanning

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

4.4.3 Vulnerability scanning

There are no NWDAF specific additions 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