3GPP TS 33.326 V19.0.0 (2025-10)

Technical Specification

3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Security Assurance Specification (SCAS) for the Network Slice-Specific Authentication and Authorization Function (NSSAAF) network product class (Release 19)

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

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 NSSAAF 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 NSSAAF 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 33.501: "Security architecture and procedures for 5G system".

[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".

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 NSSAAF-specific security requirements and related test cases

4.1 Introduction

NSSAAF specific security requirements include both requirements derived from NSSAAF security functional requirements as well as security requirements derived from threats specific to eNB as described in TR 33.926 [4]. Generic security requirements and test cases common to other network product classes have been captured in TS 33.117 [3] and are not repeated in the present document.

4.2 NSSAAF-specific security functional requirements and related test cases

4.2.1 Routes the S-NSSAI to the right place

Requirement Name: Routes the S-NSSAI to the right place

Requirement Reference: TS 33.501 [2], clause 6.8.1.2.3

Requirement Description: If the AAA-P is present (e.g. because the AAA-S belongs to a third party and the operator deploys a proxy towards third parties), the NSSAAF forwards the EAP ID Response message to the AAA-P, otherwise the NSSAAF forwards the message directly to the AAA-S. NSSAAF routes to the AAA-S based on the S-NSSAI, as specified in TS 33.501 [2], clause 6.13.

Threat Reference: TR 33.926 [4], clause P.3.2 – Threats related to NSSAAF.

Test Name: TC_NSSAAF_CORRECT_ROUTING

Purpose:

Verify that the NSSAAF forwards the NSSAA request to the right receiving end.

Pre-Conditions:

- Test environment with AMF, AAA-S and AAA-P, which may be simulated. The NSAAF under test is connected with AMF, AAA-S and AAA-P.
- A document describes the logic how the NSSAAF selects an AAA-S or AAA-P based on S-NSSAI.
- Preconfigure the NSSAAF under test with two routing entries, each for a NSSAI. One of the slice is a part of MNO and the AAA-S can be directly found by the NSSAAF, while the other slice serves 3rd party and the AAA-P will be used for NSSAA procedure.

Execution Steps

1. The AMF sends Nssaaf_NSSAA_Authenticate Req to the NSSAAF including one of the S-NSSAI.
2. The NSSAAF sends AAA message to an AAA-P.
3. Repeat step 1 and 2 with the other S-NSSAI, and the NSSAAF sends AAA message to an AAA-S.

Expected Results:

The NSSAAF forwards the NSSAA request to the correct AAA-S or AAA-P on the S-NSSAI.

Expected format of evidence:

Save the logs and the communication flow in a .pcap file.

4.2.2 AAA-S authorization in re-authentication and revocation scenarios

Requirement Name: AAA-S authorization in re-authentication and revocation scenarios

Requirement Reference: TS 33.501 [2], clause 16.4

Requirement Description: The NSSAAF checks whether the AAA-S is authorized to request the re-authentication and re-authorization by checking the local configuration of AAA-S address per S-NSSAI. If success, the NSSAAF requests UDM for the AMF serving the UE using the Nudm_UECM_Get (GPSI, AMF Registration) service operation. The UDM provides the NSSAAF with the AMF ID of the AMF serving the UE as specified in TS 33.501 [2], clause 6.13.

Threat Reference: TR 33.926 [4], clause P.3.2 – Threats related to NSSAAF.

Test Name: TC_NSSAAF_AAAS_AUTHORIZATION_REAUTH_REVOCATION

Purpose:

Verify that the AAA-S is authorized to send the re-authentication or revocation.

Pre-Conditions:

- Test environment with AAA-S and AAA-P, which may be simulated. The NSAAF under test is connected with AAA-S and AAA-P.
- A document describes the mapping between S-NSSAI and AAA-S server.

Execution Steps

1. The AAA-S sends Re-authentication or revocation message to the NSSAAF including the S-NSSAI and the GPSI.
2. The NSSAAF checks whether the AAA-S can be matched against with the S-NSSAI based on the mapping table.

Expected Results:

The NSSAAF rejects the re-authentication or revocation when the AAA-S and S-NSSAI are not mapped.

The NSSAAF passes the re-authentication or revocation when the AAA-S and S-NSSAI are mapped.

Expected format of evidence:

Save the logs and the communication flow in a .pcap file.

4.2.3 Technical baseline

4.2.3.1 Introduction

The present clause provides baseline technical requirements.

4.2.3.2 Protecting data and information

4.2.3.2.1 Protecting data and information – general

There are no NSSAAF additions to clause 4.2.3.2.1 of TS 33.117 [3].

4.2.3.2.2 Protecting data and information – unauthorized viewing

There are no NSSAAF additions to clause 4.2.3.2.2 of TS 33.117 [3].

4.2.3.2.3 Protecting data and information in storage

There are no NSSAAF additions to clause 4.2.3.2.3 of TS 33.117 [3].

4.2.3.2.4 Protecting data and information in transfer

There are no NSSAAF additions to clause 4.2.3.2.4 of TS 33.117 [3].

4.2.3.2.5 Logging access to personal data

There are no NSSAAF additions to clause 4.2.3.2.5 of TS 33.117 [3].

4.2.3.3 Protecting availability and integrity

There are no NSSAAF additions to clause 4.2.3.3 of TS 33.117 [3].

4.2.3.4 Authentication and authorization

4.2.3.4.1 Authentication attributes

There are no NSSAAF additions to clause 4.2.3.4.1 of TS 33.117 [3].

4.2.3.5 Protecting sessions

There are no NSSAAF additions to clause 4.2.3.5 of TS 33.117 [3].

4.2.3.6 Logging

There are no NSSAAF additions to clause 4.2.3.6 of TS 33.117 [3].

4.2.4 Operating systems

There are no NSSAAF additions to clause 4.2.4 of TS 33.117 [3].

4.2.5 Web servers

There are no NSSAAF additions to clause 4.2.5 of TS 33.117 [3].

4.2.6 Network devices

4.2.6.1 Protection of data and information

There are no NSSAAF additions to clause 4.2.6 of TS 33.117 [3].

4.2.6.2 Protecting availability and integrity

4.2.6.2.1 Packet filtering

There are no NSSAAF additions to clause 4.2.6.2.1 of TS 33.117 [3].

4.2.6.2.2 Interface robustness requirements

There are no NSSAAF additions to clause 4.2.6.2.2 of TS 33.117 [3].

4.2.6.2.3 GTP-C Filtering

The requirement and testcase in clause 4.2.6.2.3 of TS 33.117 [3] is not applicable to eNB network product.

4.2.6.2.4 GTP-U Filtering

There are no NSSAAF additions to clause 4.2.6.2.4 of TS 33.117 [3].

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

4.3.1 Introduction

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

4.3.2 Technical Baseline

There are no NSSAAF additions to clause 4.3.2 of TS 33.117 [3].

4.3.3 Operating Systems

There are no NSSAAF additions to clause 4.3.3 of TS 33.117 [3].

4.3.4 Web Servers

There are no NSSAAF additions to clause 4.3.4 of TS 33.117 [3].

4.3.5 Network Devices

There are no NSSAAF additions to clause 4.3.5 of TS 33.117 [3].

4.3.6 Network Functions in service-based architecture

There are no NSSAAF additions to clause 4.3.6 of TS 33.117 [3].

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

There are no NSSAAF additions to clause 4.4 of TS 33.117 [3].

Annex A (informative): Change history

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
2021-09	SA#93e	SP-210853				Presented for information and approval	1.0.0
2021-09	SA#93e					EditHelp review and upgrade to change control version	17.0.0
2023-06	SA#100	SP-230604	0001	-	F	SCAS release reference corrections	18.0.0
2025-09	SA#109	SP-251021	0003	-	F	Revision of 33.326 Rel 18	18.1.0
2025-10	-	-	-	-	-	Update to Rel-19 version (MCC)	**19.0.0**