ETSI TS 133 519 V16.2.0 (2021-01)

5G;
5G Security Assurance Specification (SCAS)
for the Network Exposure Function (NEF)
network product class
(3GPP TS 33.519 version 16.2.0 Release 16)

Reference
RTS/TSGS-0333519vg20

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 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status.
Information on the current status of this and other ETSI documents is available at
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.
The content of the PDF version shall not be modified without the written authorization of ETSI.
The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2021.
All rights reserved.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members.
3GPP™ and **LTE™** 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.

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is 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 Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, 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.

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 under http://webapp.etsi.org/key/queryform.asp.

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

Intellectual Property Rights 2
Legal Notice 2
Modal verbs terminology 2
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 NEF-specific security requirements and related test cases 7
4.1 Introduction 7
4.2 NEF-specific security functional adaptations of requirements and related test cases 7
4.2.0 Introduction 7
4.2.1 Void 7
4.2.2 Security functional requirements on the NEF deriving from 3GPP specifications and related test cases 7
4.2.2.0 General 7
4.2.2.1 Security functional requirements on the NEF deriving from 3GPP specifications – TS 33.501 [2] 7
4.2.3 Technical Baseline 9
4.2.3.1 Introduction 9
4.2.3.2 Protecting data and information 9
4.2.3.2.1 Protecting data and information – general 9
4.2.3.2.2 Protecting data and information – unauthorized viewing 9
4.2.3.2.3 Protecting data and information in storage 9
4.2.3.2.4 Protecting data and information in transfer 9
4.2.3.2.5 Logging access to personal data 10
4.2.3.3 Protecting availability and integrity 10
4.2.3.4 Authentication and authorization 10
4.2.3.5 Protecting sessions 10
4.2.3.6 Logging 10
4.2.4 Operating Systems 10
4.2.5 Web Servers 10
4.2.6 Network Devices 10
4.2.7 Void 10
4.3 NEF-specific adaptations of hardening requirements and related test cases 10
4.3.1 Introduction 10
4.3.2 Technical baseline 10
4.3.3 Operating systems 10
4.3.4 Web servers 11
4.3.5 Network devices 11
4.3.6 Network functions in service-based architecture 11
4.4 NEF-specific adaptations of basic vulnerability testing requirements and related test cases 11
Annex A (informative): Change history 12
History 13

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 NEF network product class. It refers to the Catalogue of General Security Assurance Requirements and formulates specific adaptions of the requirements and test cases given there, as well as specifying requirements and test cases unique to the NEF 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 TS 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 33.501 (Release 15): "Security architecture and procedures for 5G system".

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

[4] 3GPP TS 33.122: " Security aspects of Common API Framework (CAPIF) for 3GPP northbound APIs".

[5] 3GPP TR 33.926: "Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes".

[6] 3GPP TS 33.117: "Catalogue of general security assurance requirements".

3 Definitions of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in 3GPP 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 3GPP TR 21.905 [1].

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP 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 3GPP TR 21.905 [1].

CAPIF	Common API Framework for 3GPP northbound APIs
NEF	Network Exposure Function

4 NEF-specific security requirements and related test cases

4.1 Introduction

NEF specific security requirements include both requirements derived from NEF-specific security functional requirements as well as security requirements derived from threats specific to NEF as described in TR 33.926 [5]. Generic security requirements and test cases common to other network product classes have been captured in TS 33.117 [6] and are not repeated in the present document.

4.2 NEF-specific security functional adaptations of requirements and related test cases

4.2.0 Introduction

The present clause describes the security functional requirements and the corresponding test cases for NEF network product class. The proposed security requirements are classified in two groups:

- Security functional requirements derived from TS 33.501 [2] and detailed in clause 4.2.2.
- General security functional requirements which include requirements not already addressed in TS 33.501 [2] but whose support is also important to ensure that NEF conforms to a common security baseline detailed in clause 4.2.3.

4.2.1 Void

4.2.2 Security functional requirements on the NEF deriving from 3GPP specifications and related test cases

4.2.2.0 General

The general approach in TS 33.117 [3] clause 4.2.2.1 and all the requirements and test cases in TS 33.117 [3] clause 4.2.2.2 related to SBA/SBI aspect apply to the NEF network product class.

4.2.2.1 Security functional requirements on the NEF deriving from 3GPP specifications – TS 33.501 [2]

4.2.2.1.1 Authentication on application function

Requirement Name: Authentication on application function

Requirement Reference: TS 33.501 [2], clause 5.9.2.3, and clause 12.2

Requirement Description: "Mutual authentication between the NEF and Application Function shall be supported" as specified in TS 33.501 [2], clause 5.9.2.3. "For authentication between NEF and an Application Function that resides outside the 3GPP operator domain, mutual authentication based on client and server certificates shall be performed between the NEF and AF using TLS" and "Certificate based authentication shall follow the profiles given in 3GPP TS 33.210 [3], clause 6.2." as specified in TS 33.501 [2], clause 12.2.

Threat References: TR 33.926 [5], clause I.2.2.1, No authentication on application function

Test Case*:*

Test Name: TC_CP_AUTH_AF_NEF

Purpose: To verify that the NEF can authenticate application function and establish TLS connection towards the application server with certificate based authentication, and may authenticate application function and establish TLS connection towards the application server with pre-shared key based authentication.

Pre-Condition:

- The NEF network product shall be connected in emulated/real network environments.
- In order to establish TLS connections to the NEF network product, the application function shall offer a feature that is supported by the NEF network product, including protocol version and combination of cryptographic algorithms.
- The application function and the NEF network product shall support certificate based authentication, and may support pre-shared key based authentication.
- If the NEF network product does not support CAPIF as specified in clause 6.2.5.1 in TS 23.501 [3], the certificates or the pre-shared key shall be provisioned in the NEF network product.
- If the NEF network product supports CAPIF, the certificates or the pre-shared key shall be provisioned in the CAPIF core function, the CAPIF core function shall be able to select appropriate authentication method as defined in the sub-clause 6.5.2 in TS 33.122 [4].

Execution Steps:

1. If certificate based authentication is used, provision correct certificate on the application function, if pre-shared key based authentication is used, provision same pre-shared key on the application function.
2. The application function shall initiate establishment of TLS connection towards the NEF network product, and check whether a TLS connection is established successfully.
3. If certificate based authentication is used, provision incorrect certificate on the application function, if pre-shared key based authentication is used, provision different pre-shared key on the application function.
4. The application function shall initiate establishment of TLS connection towards the NEF network product, and check whether no new TLS connection is established.

Expected Results:

Only one TLS connection is established at step 2.

Expected format of evidence:

Evidence suitable for the interface, e.g., Screenshot containing the operational results.

4.2.2.1.2 Authorization on northbound APIs

Requirement Name: Authorization on application function

Requirement Reference: TS 33.501 [2], clause 12.4

Requirement Description: "The NEF shall authorize the requests from Application Function using OAuth-based authorization mechanism, the specific authorization mechanisms shall follow the provisions given in RFC 6749 [43]" as specified in TS 33.501 [2], clause 12.4.

Threat References: TR 33.926 [5], clause I.2.2.2, No authorization on northbound APIs

Test Case*:*

Test Name: TC_CP_AUTHOR_AF_NEF

Purpose: To verify that the NEF can authorize application function.

Pre-Condition:

- The NEF network product shall be connected in emulated/real network environments.
- The application function and the NEF network product shall support OAuth-based authorization mechanism.

- An authorization server (e.g. NRF, or CAPIF core function) that supports OAuth2 protocol to authorize NEF northbound APIs using the "Client Credentials" authorization grant has been deployed.
- The TLS connection between the NEF network product and the application function has been established.
- The authorization server is configured to grant the application function to access a northbound API of the NEF network product, called NEF northbound API A.

Execution Steps:

Test 1: without token:

1. The application function invokes Obtain_Authorization service towards the authorization server to get a token from the authorization server for accessing the NEF northbound API A.
2. The application function invokes NEF northbound API A.
3. The tester triggers the application function to invoke another northbound API of the NEF network product, called NEF northbound API B, without token.

Test 2: With incorrect token:

1. The application function invokes Obtain_Authorization service towards the authorization server to get a token from the authorization server for accessing the NEF northbound API A.
2. The application function invokes NEF northbound API A.
3. The tester triggers the application function to invoke the NEF northbound API B with a fake token.

Expected Results:

The invoking of NEF northbound API A succeeds, while the invoking of NEF northbound API B fails.

Expected format of evidence:

Evidence suitable for the interface, e.g., Screenshot containing the operational results.

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 NEF-specific additions to clause 4.2.3.2.1 of TS 33.117 [6].

4.2.3.2.2 Protecting data and information – unauthorized viewing

There are no NEF-specific additions to clause 4.2.3.2.2 of TS 33.117 [6].

4.2.3.2.3 Protecting data and information in storage

There are no NEF-specific additions to clause 4.2.3.2.3 of TS 33.117 [6].

4.2.3.2.4 Protecting data and information in transfer

There are no NEF-specific additions to clause 4.2.3.2.4 of TS 33.117 [6].

4.2.3.2.5 Logging access to personal data

There are no NEF-specific additions to clause 4.2.3.2.5 of TS 33.117 [6].

4.2.3.3 Protecting availability and integrity

There are no NEF-specific additions to clause 4.2.3.3 of TS 33.117 [6].

4.2.3.4 Authentication and authorization

There are no NEF-specific additions to clause 4.2.3.4 of TS 33.117 [6].

4.2.3.5 Protecting sessions

There are no NEF-specific additions to clause 4.2.3.5 of TS 33.117 [6].

4.2.3.6 Logging

There are no NEF-specific additions to clause 4.2.3.6 of TS 33.117 [6].

4.2.4 Operating Systems

There are no NEF-specific additions to clause 4.2.4 of TS 33.117 [6].

4.2.5 Web Servers

There are no NEF-specific additions to clause 4.2.5 of TS 33.117 [6].

4.2.6 Network Devices

There are no NEF-specific additions to clause 4.2.6 of TS 33.117 [6].

4.2.7 Void

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

4.3.1 Introduction

The requirements proposed hereafter (with the relative test cases) aim to securing NEF by reducing its surface of vulnerability. In particular, the identified requirements aim to ensure that all the default configurations of NEF (including operating system software, firmware and applications) are appropriately set.

4.3.2 Technical baseline

There are no NEF-specific additions to clause 4.3.2 of TS 33.117 [6].

4.3.3 Operating systems

There are no NEF-specific additions to clause 4.3.3 of TS 33.117 [6].

4.3.4 Web servers

There are no NEF-specific additions to clause 4.3.4 of TS 33.117 [6].

4.3.5 Network devices

There are no NEF-specific additions to clause 4.3.5 of TS 33.117 [6].

4.3.6 Network functions in service-based architecture

There are no NEF-specific additions to clause 4.3.6 of TS 33.117 [6].

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

There are no NEF-specific additions to clause 4.4 of TS 33.117 [6].

Annex A (informative): Change history

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
2019-09	SA#85					Change control version	16.0.0
2019-10						EditHelp review	16.0.1
2019-12	SA#86	SP-191138	0002	1	F	Corrections for clean-up and alignment	16.1.0
2020-12	Sa#90E	SP-201004	0003	-	F	Reference of general SBA/SBI aspect in 33.519	16.2.0

History

Document history		
V16.1.0	October 2020	Publication
V16.2.0	January 2021	Publication