

ETSI TS 133 518 V16.2.0 (2020-08)



**5G;
5G Security Assurance Specification (SCAS) for the Network
Repository Function (NRF) network product class
(3GPP TS 33.518 version 16.2.0 Release 16)**



Reference

DTS/TSGS-0333518vg20

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/CommitteeSupportStaff.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 2020.

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 NRF-specific security requirements and related test cases	7
4.1 Introduction	7
4.2 NRF-specific adaptations of security functional requirements and related test cases	7
4.2.1 Introduction.....	7
4.2.2 Security functional requirements on the NRF deriving from 3GPP specifications and related test cases.....	7
4.2.2.1 Security functional requirements on the NRF deriving from 3GPP specifications – general approach.....	7
4.2.2.2 NF discovery procedure	7
4.2.2.2.1 NF discovery authorization for specific slice	7
4.2.3 Technical Baseline	8
4.2.3.1 Introduction	8
4.2.3.2 Protecting data and information.....	8
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	9
4.2.3.3 Protecting availability and integrity.....	9
4.2.3.4 Authentication and authorization.....	9
4.2.3.5 Protecting sessions	9
4.2.3.6 Logging	9
4.2.4 Operating Systems	9
4.2.5 Web Servers.....	9
4.2.6 Network Devices	9
4.3 NRF-specific adaptations of hardening requirements and related test cases	9
4.3.1 Introduction.....	9
4.3.2 Technical baseline.....	10
4.3.3 Operating systems.....	10
4.3.4 Web servers	10
4.3.5 Network devices	10
4.3.6 Network functions in service-based architecture	10
4.4 NRF-specific adaptations of basic vulnerability testing requirements and related test cases	10
Annex A (informative): Change history	11
History	12

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 objectives, requirements and test cases that are specific to the NRF network product class. It refers to the Catalogue of General Security Assurance Requirements and formulates specific adaptations of the requirements and test cases given there, as well as specifying requirements and test cases unique to the NRF 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 33.117: "Catalogue of general security assurance requirements".
- [3] 3GPP TS 33.501 v15: "Security architecture and procedures for 5G system".
- [4] 3GPP TS 23.502: "Procedures for the 5G System".
- [5] 3GPP TS 29.510: "5G System; Network function repository services; Stage 3".
- [6] 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 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].

NF	Network Function
NRF	Network Repository Function

4 NRF-specific security requirements and related test cases

4.1 Introduction

NRF specific security requirements include both requirements derived from NRF-specific security functional requirements in relevant specifications as well as the security requirements introduced in the present document derived from the threats specific to NRF as described in TR 33.926 [6].

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

4.2.1 Introduction

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

- Security functional requirements derived from TS 33.501 [3] and detailed in clause 4.2.2.
- General security functional requirements which include requirements not already addressed in TS 33.501 [3] but whose support is also important to ensure that NRF conforms to a common security baseline detailed in clause 4.2.3.

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

4.2.2.1 Security functional requirements on the NRF deriving from 3GPP specifications – general approach

In addition to the requirements and test cases in TS 33.117 [2], clause 4.2.2, a NRF shall satisfy the following:

It is assumed for the purpose of the present SCAS that a NRF conforms to all mandatory security-related provisions pertaining to a NRF in:

- 3GPP TS 33.501 [3]: "Security architecture procedures for 5G system";
- other 3GPP specifications that make reference to TS 33.501 [3] or are referred to from TS 33.501 [3].

Security procedures pertaining to a NRF are typically embedded in NF discovery/registration/access token request procedures and are hence assumed to be tested together with them.

4.2.2.2 NF discovery procedure

4.2.2.2.1 NF discovery authorization for specific slice

Requirement Name: NF discovery authorization for specific slice

Requirement Reference: TS 33.501 [3], clause 5.9.2.1, TS 23.502 [4], clause 4.17.4, and TS 29.510 [5], clause 6.2.3.2.3.1.

Requirement Description:

"NRF shall be able to ensure that NF Discovery and registration requests are authorized" as specified in TS 33.501 [3], clause 5.9.2.1.

"The NRF authorizes the Nnrf_NFDiscovery_Request. Based on the profile of the expected NF/NF service and the type of the NF service consumer, the NRF determines whether the NF service consumer is allowed to discover the expected NF instance(s). If the expected NF instance(s) or NF service instance(s) are deployed in a certain network slice, NRF authorizes the discovery request according to the discovery configuration of the Network Slice, e.g. the expected NF instance(s) are only discoverable by the NF in the same network slice".

as specified in TS 23.502 [4], clause 4.17.4.

"If included, the requester-snsais IE shall contain the list of S-NSSAI of the requester NF. The NRF shall use this to return only those NF profiles of NF Instances allowing to be discovered from the slice(s) identified by this IE, according to the "allowedNssais" list in the NF Profile and NF Service" as specified in TS 29.510 [5], clause 6.2.3.2.3.1.

Threat References: TR 33.926 [6], clause H.2.2.1, No slice specific authorization for NF discovery

Test Case:

Test Name: TC_DISC_AUTHORIZATION_SLICE_NRF

Purpose:

Verify that the NRF under test does not authorize slice specific discovery request for the NF instance which is not part of the requested slice, according to the slice specific discovery configuration of the requested NF instance.

Procedure and execution steps:

Pre-Conditions:

- Test environment with the NF1 and NF2, which may be simulated.
- The NF2 is configured with a list of S-NSSAI, which contains slice A but not slice B.
- The NF1 is configured as a NF instance belonging to slice B and is connected in emulated/real network environment.
- The NF1 and NF2 is successfully authenticated with the NRF under test.

Execution Steps

1. The NF2 registers at the NRF under test with a list of S-NSSAI.
2. The NF1 sends an Nnrf_NFDiscovery_Request to the NRF under test with the expected service name of NF2, NF type of the expected NF2.
3. The NRF under test determines that NF2 instance only allows discovery from NFs belonging to slice A, according to the "allowedNssais" list stored in NF2 Profile.

Expected Results:

The NRF under test returns a response with "403 Forbidden" status code, as specified in clause 5.3.2.2.2 of TS 29.510 [5].

Expected format of evidence:

Evidence suitable for the interface, e.g., evidence can be presented in the form of screenshot/screen-capture.

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 NRF-specific additions to clause 4.2.3.2.1 of TS 33.117 [2].

4.2.3.2.2 Protecting data and information – unauthorized viewing

There are no NRF-specific additions to clause 4.2.3.2.2 of TS 33.117 [2].

4.2.3.2.3 Protecting data and information in storage

There are no NRF-specific additions to clause 4.2.3.2.3 of TS 33.117 [2].

4.2.3.2.4 Protecting data and information in transfer

There are no NRF-specific additions to clause 4.2.3.2.4 of TS 33.117 [2].

4.2.3.2.5 Logging access to personal data

There are no NRF-specific additions to clause 4.2.3.2.5 of TS 33.117 [2].

4.2.3.3 Protecting availability and integrity

There are no NRF-specific additions to clause 4.2.3.3 of TS 33.117 [2].

4.2.3.4 Authentication and authorization

There are no NRF-specific additions to clause 4.2.3.4 of TS 33.117 [2].

4.2.3.5 Protecting sessions

There are no NRF-specific additions to clause 4.2.3.5 of TS 33.117 [2].

4.2.3.6 Logging

There are no NRF-specific additions to clause 4.2.3.6 of TS 33.117 [2].

4.2.4 Operating Systems

There are no NRF-specific additions to clause 4.2.4 of TS 33.117 [2].

4.2.5 Web Servers

There are no NRF-specific additions to clause 4.2.5 of TS 33.117 [2].

4.2.6 Network Devices

There are no NRF-specific additions to clause 4.2.6 of TS 33.117 [2].

4.3 NRF-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 NRF by reducing its surface of vulnerability. In particular, the identified requirements aim to ensure that all the default configurations of NRF (including operating system software, firmware and applications) are appropriately set.

4.3.2 Technical baseline

All text from TS 33.117, clause 4.3.2 also applies to NRFs. There are no NRF-specific adaptations or additions to clause 4.3.2 of TS 33.117 [2].

4.3.3 Operating systems

There are no NRF-specific additions to clause 4.3.3 of TS 33.117 [2].

4.3.4 Web servers

There are no NRF-specific additions to clause 4.3.4 of TS 33.117 [2].

4.3.5 Network devices

There are no NRF-specific additions to clause 4.3.5 of TS 33.117 [2].

4.3.6 Network functions in service-based architecture

There are no NRF-specific additions to clause 4.3.6 in TS 33.117 [2].

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

All text from TS 33.117, clause 4.4 also applies to NRFs. There are no NRF-specific adaptations or additions to clause 4.4 of TS 33.117 [2].

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	0001	-	F	Adding abbreviations and corrections for alignment	16.1.0
2020-07	SA#88E	SP-200358	0002	1	F	Update to the test case of NF discovery authorization for specific slice	16.2.0

History

Document history		
V16.2.0	August 2020	Publication