3GPP TS 33.518 V19.0.0 (2025-07)

Technical Specification

3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 5G Security Assurance Specification (SCAS) for the Network Repository Function (NRF) network product class (Release 19)

Keywords
5G, SCAS,NRF, security

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....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 based on expected NF profile....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....10
4.2.3.2.4 Protecting data and information in transfer....10
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
4.3 NRF-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....11
4.3.4 Web servers....11
4.3.5 Network devices....11
4.3.6 Network functions in service-based architecture....11
4.4 NRF-specific adaptations of basic vulnerability testing requirements and related test cases....11

4.4.1 Introduction....11
4.4.2 Port Scanning....11
4.4.3 Vulnerability scanning....11
4.4.4 Robustness and fuzz testing....11

Annex A (informative): Change 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 adaptions 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: "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".

[7] 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 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 based on expected NF profile

Requirement Name: NF discovery authorization for specific scopes

Requirement Reference: TS 33.501 [3], clause 13.3.1.3, TS 23.502 [4], clause 4.17.4, and TS 29.510 [5], clause 6.2.3.2.3.1.

Requirement Description:

NRF is expected to 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 checks that the values of the authorization parameters in the NF (Service) Profile of an NF Service Producer allows an NF Service Consumer to discover the NF Service Producer. In the response message, the NRF only returns information of those NF Service Producer instances that the NF Service Consumer is authorized to discover, as specified in the TS 33.501 [3], clause 13.3.1.3.

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.

Based on operator's policies, a discovery request not including the requester's information necessary to validate the authorization parameters in NF Profiles can be rejected or accepted but with only returning in the discovery response NF Instances whose authorization parameters allow any NF Service Consumer to access their services. The authorization parameters in NF Profile are those used by NRF to determine whether a given NF Instance / NF Service Instance can be discovered by an NF Service Consumer in order to consume its offered services (e.g. "allowedNfTypes", "allowedNfDomains", etc.), as specified in TS 29.510 [5], clause 6.2.3.2.3.1, Note 12.

If included, the requester-snssais IE is expected to contain the list of S-NSSAI of the requester NF. The NRF is expected to 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 Authorization of NF discovery based on Authorization Parameters

Test Case:

Test Name: TC_DISC_AUTHORIZATION_ALLOWED_PARAMETER

Purpose:

Ensure that the NRF being tested does not authorize a discovery request from an NF service consumer instance that lacks the correct authorization provided in the request, based on the parameters prefixed with “allowed” (e.g., allowedNfTypes, allowedNfDomains, allowedNssais…) provided by the NF service producer profile.

Procedure and execution steps:

Pre-Conditions:

- Test environment with the NF1 and NF2, which may be simulated. The NF2 will attempt to discover NF1.
- The NRF documentation provides information on whether unauthorized requests are rejected or accepted, but only returns NF Instances in the discovery response whose service the NF service consumer is authorized to access. If this is configurable, the tester is required to test both options.
- If the NRF under test does not support parameters from the allowedList in the table below, the test steps regarding these parameters are not applicable.

Execution Steps

For all Test Case specific parameters defined in the table 4.2.2.2.1-1, the tester shall repeat the following execution steps.

Table 4.2.2.2.1-1 Test Case Specific Parameter Sets

Test Case	*parameter NF1*	*parameter NF2*	*allowedList (NF1)*	*requester-type (NF2)*
A	NfType NF1	NfType NF2	allowedNfTypes	requester-nf-type
B	PLMN NF1	PLMN NF2	allowedPlmns	requester-plmn-list
C	FQDN NF1	FQDN NF2	allowedNfDomains	requester-nf-instance-fqdn
D	SNPN NF1	SNPN NF2	allowedSnpns	requester-snpn-list
E	S-NSSAI NF1	S-NSSAI NF2	allowedNssais	requester-snssais
F	S-NSSAI NF1 and PLMN NF1	S-NSSAI NF2 and PLMN NF2	allowedPlmns	requester-plmn-specific-snssai-list

1. The tester configures NF1 with *parameter NF1* and NF2 with *parameter NF2*, where the two parameter values are different. The tester should select the mandatory and optional profile parameters for NF1 and NF2 such that they do not conflict with other authorization test cases in this section.

2. The tester configures NF1 to ensure that it is not accessible by NF2 by disallowing *parameter NF2* via the *allowedList parameter* in the profile NF1.

3. The tester triggers NF1 to register as a new NF instance via the NFManagement API at the NRF under test.

4. The tester triggers NF2 to send an Nnrf_NFDiscovery_Request message to the NRF under test with *target-nf-type* set to NfType NF1 and *requester-type parameter* set to the corresponding *parameter NF2*.

Expected Results:

If the NRF under test is configured to reject unauthorized requests, the NRF responds with a "403 Forbidden" status code, as specified in clause 5.3.2.2.2 of TS 29.510 [5].

If the NRF under test is configured to accept unauthorised requests, but only returns NF instances whose authorisation is accepted in the discovery response, the discovery response will not contain any information about the NF1.

Expected format of evidence:

Evidence suitable for the interface, e.g., evidence can be presented in the form of packet trace (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 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

4.4.1 Introduction

There are no NRF specific addtions to clause 4.4.1 of TS 33.117 [2].

4.4.2 Port Scanning

There are no NRF specific addtions to clause 4.4.2 of TS 33.117 [2].

4.4.3 Vulnerability scanning

There are no NRF specific addtions to clause 4.4.3 of TS 33.117 [2].

4.4.4 Robustness and fuzz testing

The test cases under clause 4.4.4 of TS 33.117 [2] are applicable to NRF.

The interface defined for the NRF are in 4.2.3 of TS 23.501 [7].

According to clause 4.4.4 of TS 33.117 [2], 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 NRF, the following interface and protocols are in the scope of the testing:

- For Nnrf: 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 [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
2022-03	-	-	-	-	-	Update to Rel-17 version (MCC)	17.0.0
2023-06	SA#100	SP-230677	0003	1	B	Robustness interfaces and protocols defined for NRF	18.0.0
2023-06	SA#100	SP-230677	0004	-	F	SCAS release reference corrections	18.0.0
2025-07	SA#108	SP-250657	0008	1	F	NF discovery authorization based on expected NF profile	19.0.0