3GPP TS 33.522 V19.0.0 (2025-10)

Technical Specification

3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 5G Security Assurance Specification (SCAS); Service Communication Proxy (SCP) (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.....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.....7
4 SCP-specific security requirements and related test cases.....7
4.1 Introduction.....7
4.2 SCP-specific adaptations of security functional requirements and related test cases.....7
4.2.1 Introduction.....7
4.2.2 Security functional requirements on the SCP derived from 3GPP specifications and related test cases.....7
4.2.2.1 Security functional requirements on the SCP derived from 3GPP specifications – general approach.....7
4.2.2.2 Security functional requirements of SBI aspects.....8
4.2.2.2.1 Introduction.....8
4.2.2.2.2 Protection at the transport layer.....8
4.2.2.2.3 Authorization of NF service access.....8
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.....8
4.2.3.2.2 Protecting data and information – unauthorized viewing.....8
4.2.3.2.3 Protecting data and information in storage.....8
4.2.3.2.4 Protecting data and information in transfer.....8
4.2.3.2.5 Logging access to personal data.....8
4.2.3.3 Protecting availability and integrity.....8
4.2.3.4 Authentication and authorization.....8
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 SCP-specific adaptations of hardening requirements and related test cases.....9
4.3.1 Introduction.....9
4.3.2 Technical Baseline.....9
4.3.3 Operating Systems.....9
4.3.4 Web Servers.....9
4.3.5 Network Devices.....9
4.3.6 Network Functions in service-based architecture.....9
4.4 SCP-specific adaptations of basic vulnerability testing requirements and related test cases.....9
4.4.1 Introduction.....10
4.4.2 Port Scanning.....10
4.4.3 Vulnerability scanning.....10
4.4.4 Robustness and fuzz testing.....10
Annex A (informative): Change history.....11

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 SCP 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 SCP 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 TR 23.501: "System architecture for the 5G System (5GS); Stage 2".

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

[6] 3GPP TS 23.502: "Procedures for the 5G System (5GS)".

[7] 3GPP TS 29.500: "5G System; Technical Realization of Service Based Architecture; Stage 3".

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 SCP-specific security requirements and related test cases

4.1 Introduction

The structure of the present document is aligned with TS 33.117 [2] such that the SCP-specific adaptation of a generic requirements in clause 4 of TS 33.117 [2], can always be found in clause 4 of the present document. The text on pre-requisites for testing in clause 4.1.1 of TS 33.117 [2] applies also to the present document.

SCP-specific security requirements include both requirements derived from SCP-specific security functional requirements in relevant specifications as well as security requirements introduced in the present document derived from the threats specific to SCP as described in TR 33.926 [5].

4.2 SCP-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 SCP 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 SCP conforms to a common security baseline detailed in clause 4.2.3.

4.2.2 Security functional requirements on the SCP derived from 3GPP specifications and related test cases

4.2.2.1 Security functional requirements on the SCP derived from 3GPP specifications – general approach

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

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

- TS 33.501 [3]: "Security architecture and procedures for 5G system";
- other 3GPP specifications that make reference to TS 33.501[3] or are referred to from TS 33.501 (e.g. TS 23.501 [4], TS 23.502 [6], TS 29.500 [7], etc.).

Security procedures pertaining to an SCP are typically embedded in NF/NF indirect communication, delegated discovery, message forwarding and routing, and are hence assumed to be tested together with them in interoperability testing at PLMN level, shared-slice level and slice-specific level.

4.2.2.2 Security functional requirements of SBI aspects

4.2.2.2.1 Introduction

According to TS 23.501 [4], although the SCP is not a Network Function instance and does not expose services itself, it still needs to support service-based interface. Therefore, the general baseline requirements supported by all Network Functions (NF) utilizing Service-Based Interfaces (SBI) as defined in TS 33.117 [2] clause 4.2.2.2 shall also be applicable to the SCP network product class. This clause contains SCP-specific adaptations to the general SBI requirements and related test cases.

4.2.2.2.2 Protection at the transport layer

There are no SCP-specific additions to clause 4.2.2.2.2 of TS 33.117 [2].

4.2.2.2.3 Authorization of NF service access

The SCP is not a network function instance and does not provide any services to any consumer NF. It supports OAuth 2.0 based service access authorization for NF service access, but it does not verify access tokens as NF producers do. Therefore, the requirements and test cases in clause 4.2.2.2.3 of TS 33.117 [2] are not applicable to the SCP network product class.

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 SCP-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 SCP-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 SEPP-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 SCP-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 SCP-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 SCP-specific additions to clause 4.2.3.3 of TS 33.117 [2].

4.2.3.4 Authentication and authorization

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

4.2.3.5 Protecting sessions

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

4.2.3.6 Logging

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

4.2.4 Operating Systems

There are no SCP-specific additions to clause 4.2.4 of TS 33.117 [3].

4.2.5 Web Servers

There are no SCP-specific additions to clause 4.2.5 of TS 33.117 [3].

4.2.6 Network Devices

There are no SCP-specific additions to clause 4.2.6 of TS 33.117 [3].

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

4.3.2 Technical Baseline

There are no SCP-specific additions to clause 4.3.2 in TS 33.117 [2].

4.3.3 Operating Systems

There are no SCP-specific additions to clause 4.3.3 in TS 33.117 [2].

4.3.4 Web Servers

There are no SCP-specific additions to clause 4.3.4 in TS 33.117 [2].

4.3.5 Network Devices

There are no SCP-specific additions to clause 4.3.5 in TS 33.117 [2].

4.3.6 Network Functions in service-based architecture

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

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

4.4.1 Introduction

There are no SCP specific addtions to clause 4.4.1 of TS 33.117 [3].

4.4.2 Port Scanning

There are no SCP specific addtions to clause 4.4.2 of TS 33.117 [3].

4.4.3 Vulnerability scanning

There are no SCP specific addtions 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 SCP.

The interface defined for the SCP are in clause 4.2.3 of TS 23.501 [4].

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 SCP, the following interface and protocols are in the scope of the testing:

- For SBI: 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[1**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
2021-12	SA#94e	SP-211395				Presented for information and approval	1.0.0
2021-12	SA#94e					EditHelp review and ugprade to change control	17.0.0
2022-03	SA#95e	SP-220237	0001	1	F	Reference to SCP-specific requirements	17.1.0
2022-03	SA#95e	SP-220237	0002	-	F	Reference to other 3GPP specs	17.1.0
2023-06	SA#100	SP-230677	0003	1	B	Robustness interfaces and protocols defined for SCP	18.0.0
2023-06	SA#100	SP-230677	0004	-	F	SCAS release reference corrections	18.0.0
2025-10	-	-	-	-	-	Update to Rel-19 version (MCC)	**19.0.0**