3GPP TS 33.515 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 Session
Management Function(SMF)
network product class
(Release 19)**

Keywords
5G, Security, Assurance, SMF, product, class

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 SMF 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 SMF 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 23.501: "System Architecture for the 5G System".

[2]   3GPP TS 33.117: "Catalogue of general security assurance requirements".

[3]   3GPP TS 23.060: "General Packet Radio Service".

[4]   3GPP TR 33.926: "Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes".

[5]   3GPP TS 29.281: "General Packet Radio System (GPRS) Tunnelling Protocol User Plane (GTPv1-U) ".

[6]   3GPP TS 32.255: "Charging Management; 5G Data Connectivity Domain Charging".

[7]   3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[8]   3GPP TS 33.501: "Security architecture and procedures for 5G system".

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 [7] 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 [7].

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].

CHF   Charging Function
SCAS   Security Assurance Specification
SMF   Session Management Function
TEID   Tunnel Endpoint Identifier
UDM   Unified Data Management Function

UPF	User Plane Function

4 SMF-specific security requirements and related test cases

4.1 Introduction

SMF specific security requirements include both SMF-specific security functional requirements in relevant specifications as well as security requirements introduced in the present document derived from the threats specific to SMF as described in TR 33.926 [4].

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

4.2.1 Introduction

Present clause contains SMF-specific security functional adaptations of requirements and related test cases.

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

4.2.2.1 Security functional requirements on the SMF deriving from 3GPP specifications

4.2.2.1.0 General

The general approach in TS 33.117 [2] clause 4.2.2.1 and all the requirements and test cases in TS 33.117 [2] clause 4.2.2.2 related to SBA/SBI aspect apply to the SMF network product class.

4.2.2.1.1 Priority of UP security policy

Requirement Name: Priority of UP security policy

Requirement Reference: TS 23.501 [1], clause 5.10.3

Requirement Description: User Plane Security Policy from UDM takes precedence over locally configured User Plane Security Policy as specified in TS 23.501 [1], clause 5.10.3

Threat References: TR 33.926 [4], clause J.2.2.1 Non-compliant UP security policy handling

Test Case:

Test Name: TC_UP_POLICY_PRECEDENCE_SMF

Purpose:

Verify that the user plane security policy from the UDM takes precedence at the SMF under test over locally configured user plane security policy.

Pre-Conditions:

Test environment with AMF and UDM may be simulated.

Both UDM and SMF under test are configured with UP security policy, and the UP security policies are different.

There is no Session Management Subscription data in SMF.

Execution Steps

1) The tester triggers PDU session establishment procedure by sending Nsmf_PDUSession_CreateSMContext Request message to the SMF.

2) The SMF under test retrieves the Session Management Subscription data using Nudm_SDM_Get service from UDM, where the Session Management Subscription data includes the user plane security policy stored in UDM.

3) The tester captures the Namf_Communication_N1N2MessageTransfer message sent from the SMF under test to the AMF.

Expected Results:

There is a Security Indication IE in the N2 SM information contained in the Namf_Communication_N1N2MessageTransfer message, which is the same with the UP security policy configured in the UDM.

Expected format of evidence:

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

4.2.2.1.2 Void

4.2.2.1.3 Security functional requirements on the SMF checking UP security policy

Requirement Name: UP security policy check.

Requirement Reference: TS 33.501 [8], clause 6.6.1

Requirement Description: According to TS 33.501 [8], clause 6.6.1, the SMF verifies that the UE's UP security policy received from the target ng-eNB/gNB is the same as the UE's UP security policy that the SMF has locally stored. If there is a mismatch, the SMF sends its locally stored UE's UP security policy of the corresponding PDU sessions to the target gNB. This UP security policy information, if included by the SMF, is delivered to the target ng-eNB/gNB in the Path-Switch Acknowledge message. The SMF logs capabilities for this event and may take additional measures, such as raising an alarm.

Threat References: TR 33.926 [4], clause J.2.2.4, Unchecked UP security policy.

TEST CASE:

Test Name: TC_UP_SECURITY_POLICY_SMF

Purpose:

Verify that the SMF checks the UP security policy that is sent by the ng-eNB/gNB during handover.

Pre-Conditions:

The SMF under test is preconfigured with a UE UP security policy.

Execution

1. The tester sends the Nsmf_PDUSession_UpdateSMContext Request message to the SMF under test. A UE UP security policy different than the one preconfigured at the SMF under test is included in the Request message.

2. The tester captures the Nsmf_PDUSession_UpdateSMContext Response message sent from the SMF under test.

Expected Results:

The preconfigured UE security policy is contained in the 'n2SmInfo' IE in the captured Response message.

Expected format of evidence:

Files containing the triggered HTTP messages (e.g. pcap trace).

4.2.2.1.4 Charging ID Uniqueness

Requirement Name: Charging ID uniqueness.

Requirement Reference: TS 32.255 [6], clause 5.1.2

Requirement Description: According to TS 32.255 [6], clause 5.1.2:

- The SMF supports PDU session charging using service based interface.

- The SMF collects charging information per PDU session for UEs served under 3GPP access and non-3GPP access.

- Every PDU session is assigned a unique identity number for billing purposes per PLMN. (i.e. the Charging Id).

Threat Reference: TR 33.926 [4], clause J.2.2.3, "Failure to assign unique Charging ID for a session"

TEST CASE:

Test Name: TC_CHARGING_ID_UNIQUENESS_SMF

Purpose:

Verify that the charging ID generated by the SMF for each PDU session is unique.

Pre-Conditions:

Test environment is set up with a Charging Function (CHF), which may be real or simulated, and the SMF under test. The tester is able to capture the traffic between the SMF under test and the CHF.

Execution Step

1) The tester intercepts the traffic between the SMF under test and the CHF.

2) The tester triggers the establishment of the maximum number of concurrent PDU sessions that the SMF under test can handle.

3) The tester captures each Charging Data Request [initial] sent from the SMF under test to the CHF, and verifies the charging ID contained in the 'PDU Session Charging Information' IE in each Charging Data Request [initial] is unique.

Expected Results:

The charging ID in each Charging Data Request [initial] is unique.

Expected format of evidence:

Files containing the Charging Data Request [initial] messages (e.g. pcap trace).

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

4.2.3.4 Authentication and authorization

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

4.2.3.5 Protecting sessions

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

4.2.3.6 Logging

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

4.2.4 Operating Systems

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

4.2.5 Web Servers

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

4.2.6 Network Devices

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

4.2.7 Void

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

4.3.1 Introduction

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

4.3.2 Technical baseline

There are no SMF-specific additions to clause 4.3.2 of TS 33.117 [2].

4.3.3 Operating systems

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

4.3.4 Web servers

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

4.3.5 Network devices

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

4.3.6 Network functions in service-based architecture

There are no SMF-specific additions to clause 4.3.6 of TS 33.117 [2].

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

4.4.1 Introduction

There are no SMF specific additions to clause 4.4.1 of TS 33.117 [2].

4.4.2 Port Scanning

There are no SMF specific additions to clause 4.4.2 of TS 33.117 [2].

4.4.3 Vulnerability scanning

There are no SMF specific additions 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 SMF.

The interfaces defined for the SMF are defined in clause 4.2.3 of TS 23.501 [1].

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 SMF, the following interfaces and protocols are in the scope of the testing:

- For Nsmf: The TCP, HTTP2 and JSON protocols.

- For N4: The UDP and PFCP 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	0003	-	F	Adding missing abbreviations	16.1.0
2019-12	SA#86	SP-191138	0004	1	F	Corrections for clean-up and alignment	16.1.0
2020-07	SA#88e	SP-200358	0005	-	F	Deletion of the test case on TEID	16.2.0
2020-12	SA#90e	SP-201004	0006	-	F	Reference of general SBA/SBI aspect in 33.515	16.3.0
2021-09	SA#93e	SP-210849	0008	1	F	Correction of message name in SMF	16.4.0
2022-03	-	-	-	-	-	Update to Rel-17 version (MCC)	17.0.0
2023-06	SA#100	SP-230677	0009	1	B	Robustness interfaces and protocols defined for SMF	18.0.0
2023-06	SA#100	SP-230677	0010	1	F	SCAS release reference corrections	18.0.0
2023-12	SA#102	SP-231339	0011	1	F	Correction of IE and protocol	18.1.0
2025-07	SA#108	SP-250657	0012	-	F	Correction of test names and clean up of 33.515	19.0.0