ETSI TS 133 515 V16.2.0 (2020-08)

5G;
5G Security Assurance Specification (SCAS)
for the Session Management Function (SMF)
network product class
(3GPP TS 33.515 version 16.2.0 Release 16)

Reference
DTS/TSGS-0333515vg20

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

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

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 (Release 15): "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 security functional adaptations of 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

4.2.2.1.1 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:

"The SMF shall verify 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 shall send 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 shall log 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_SMContextUpate 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_SMContextUpdate Response message sent from the SMF under test.

Expected Results:

The preconfigured UE security policy is contained in the ‘n2SmInf’ IE in the captured Response message.

Expected format of evidence:

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

4.2.2.1.4 Charging ID Uniqueness

Requirement Name: Charing ID uniqueness.

Requirement Reference: TS 32.255 [6], clause 5.1.2

Requirement Description: :

"- The SMF shall support PDU session charging using service based interface.

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

- Every PDU session shall be 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 Other SMF-specific adaptations of hardening requirements and related test cases

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

4.4 Network functions in service-based architecture

There are no SMF-specific 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	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

History

Document history		
V16.2.0	August 2020	Publication