ETSI TS 133 529 V19.1.0 (2026-01)

TECHNICAL SPECIFICATION

5G;
Security Assurance Specification (SCAS)
for the Short Message Service Function (SMSF)
network product class
(3GPP TS 33.529 version 19.1.0 Release 19)

Reference
DTS/TSGS-0333529vj10

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 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are 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 IPR online database.

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, 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.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**, **LTE™** and **5G™** logo 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.

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 at 3GPP to ETSI numbering cross-referencing.

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 objectives, security assurance requirements and test cases specific to the SMSF network product class. It refers to the Catalogue of General Security Assurance Requirements. It formulates specific adaptations of the requirements and test cases given in the catalogue. It also specifies requirements derived from other technical specifications and test cases unique to the SMSF 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 33.926: "Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes".

[5] 3GPP TS 23.040: "Technical realization of the Short Message Service (SMS)".

[6] 3GPP TS 23.501: "System Architecture for the 5G System (5GS)".

[7] 3GPP TS 29.540: "5G System; SMS Services".

[8] 3GPP TS 29.338: "Diameter based protocols to support Short Message Service (SMS) capable Mobile Management Entities (MMEs)".

[9] 3GPP TS 29.002: "Mobile Application Part (MAP) specification".

[10] 3GPP TS 33.210: "Network Domain Security (NDS): IP network layer security".

[11] 3GPP TS 33.310: "Network Domain Security (NDS): Authentication Framework".

[12] IETF RFC 6733: "Diameter Base Protocol".

[13] 3GPP TS 33.204: "3G Security; Network Domain Security (NDS): Transaction Capabilities Application Part (TCAP) user security".

[14] Void

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].

Diameter application nodes: Network entities, i.e. SMSC, IP-SM-GW, SMS-Router in SMS application case, that implement the Diameter protocol to establish connection with other nodes implementing Diameter protocol.

Service Center (SC): Defined in TS 23.040 [5].

Short Message (SM): Defined in TS 23.040 [5].

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].

SBI	Service Based Interface
SMSF	Short Message Service Function
UDM	Unified Data Management

4 SMSF-specific security requirements and related test cases

4.1 Introduction

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

4.2 SMSF-specific 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 SMSF network product class. Clause 4.2.7 outlines specific security functional requirements related to the non service-based interfaces of SMSF, that are not covered in TS 33.117 [2].

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

There are no SMSF-specific additions to clause 4.2.2 of TS 33.117 [2].

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

There are no SMSF-specific additions to clause 4.2.3.2 of TS 33.117 [2].

4.2.3.3 Protecting availability and integrity

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

4.2.3.4 Authentication and authorization

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

4.2.3.5 Protecting sessions

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

4.2.3.6 Logging

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

4.2.4 Operating Systems

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

4.2.5 Web Servers

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

4.2.6 Network Devices

The clause 4.2.6 of TS 33.117 [2] applies to SMSF, except for the clauses 4.2.6.2.3 and 4.2.6.2.4, which are not applicable. There are no SMSF-specific additions to clause 4.2.6 of TS 33.117 [2].

4.2.7 Security functional requirements on the SMSF– Non Service-Based Interfaces

4.2.7.1 Protection on SGd Diameter Interface between SMSF and the Diameter application node

Requirement Name: Protection data and information on SGd

Requirement Reference: TS 33.501 [3], clause 9.5, TS 33.210 [10], clause 6.2, TS 33.310 [11], clause 6.1.3a.

Requirement Description: TS 33.501 [3] mentions that protection of Diameter interface shall be supported according to NDS/IP as specified in TS 33.210 [10], unless security is provided by other means e.g. physical security. For authentication between SMSF and Diameter application node over diameter interface, mutual authentication based on client and server certificates is performed, if using TLS. Certificate based authentication follows the profiles given in TS 33.210 [10] clause 6.2, and TS 33.310 [11] clause 6.1.3a, with the restriction that it shall be compliant with the profile given by Diameter Base Protocol as defined in RFC 6733 [12], except the cipher suites. A SEG may be used to terminate the NDS/IP IPsec tunnels.

Threat References: TR 33.926 [4], clause Y.2.4.1, SMSF control data and user data protection on SGd Diameter Interface

Test Case:

Test Name: TC_Protect_Diameter_SGd

Purpose: To verify the mechanisms implemented to protect data and information in transfer to and from the SMSF's Diameter protocol-based SGd interface.

NOTE: This test case applies to the network function with SGd Diameter interface.

Pre-Conditions:

Network product documentation containing information about supported NDS/IP protocols is provided by the vendor.

A Diameter application node peer implementing the security protocol configured by the vendor shall be available.

SMSF documentation, stating which security protocols for protection of data in transit are implemented and which profiles in TS 33.310 [11] and TS 33.210 [10] are applicable, is provided by the vendor. The tester shall base the tests on the profile defined by 3GPP in Clause 6.2 of TS 33.310 [11].

For TLS/DTLS, the tester shall base the tests on the profile defined by 3GPP in Clause 6.1.3a of TS 33.310 [11] and Clause 6.2 of TS 33.210 [10], with the restriction that it shall be compliant with the profile given by Diameter Base Protocol as defined in RFC 6733 [12], except the cipher suites.

For IKE and IPsec, the tester shall base the tests on the profile defined by 3GPP in TS 33.210 [10].

Procedure and execution steps, expected results, expected format of evidence:

These are the same as for the test case in TS 33.117 [2], clause 4.2.3.2.4, excluding execution step 4, and the profiles as mentioned in requirement description shall be followed in pre-conditions.

4.2.7.2 Protection of Diameter Session on SGd Interface

Requirement Name: Diameter session on SGd interface

Requirement Reference: TS 29.338 [8], clause 4.5; RFC 6733 [12], clause 8.8

Requirement Description:

SMSF supports implicit termination of SGd Diameter application sessions. The client (server) includes in its requests (responses) the Auth-Session-State AVP set to the value NO_STATE_MAINTAINED (1), as described in IETF RFC 6733 [12]. The server sets the Auth-Session-State AVP value to NO_STATE_MAINTAINED (1), irrespective of what value the client sets. Neither the Authorization-Lifetime AVP nor the Session-Timeout AVP be present in requests or responses [8].

To protect Diameter sessions, SMSF supports the following requirements:

1. Diameter session ID AVP be unique, i.e. uniquely identify the user session and distinguish the session from all other active sessions.
2. The session ID be generated by the Diameter application node that initiates the session.

Threat References: TR 33.926 [4], clause Y.2.2.2, Diameter session information disclosure

Test Case:

Test Name: TC_DIAMETER_SGd_SESSION

Purpose:

Verify that the above Diameter session and session ID related requirements have been met.

Procedure and execution steps:

Pre-Conditions:

- This text case is applicable only if network product supports Diameter SGd Interface
- The Diameter application node uses a session ID to identify a session between the node and its peer.
- The documentation should describe the algorithm used to generate the session IDs, for details see Section 8.8 in RFC 6733 [12].

Execution Steps:

1) The tester logs in the network product.
2) The tester sends SGd application request message as follows:
   a) Auth-Session-State AVP is set to the value NO_STATE_MAINTAINED (1).
   b) Neither the Authorization-Lifetime AVP nor the Session-Timeout AVP is present in requests.
   c) The tester generates session ID as per the documentation and uses it as session ID AVP in the message.
3) The tester sends SGd application request message as follows:
   a) Auth-Session-State AVP is set to the value STATE_MAINTAINED (0).
   b) Authorization-Lifetime AVP and Session-Timeout AVP are present in request.
   c) The tester generates session ID as per the documentation and uses it as session ID AVP in the message.
4) The tester checks the response for its request message in step 2 and 3. In both cases, the tester verifies that:
   a) Auth-Session-State AVP is set to the value NO_STATE_MAINTAINED (1).
   b) Neither the Authorization-Lifetime AVP nor the Session-Timeout AVP is present in response.
   c) The session IDs in two request messages are different and unique.
5) The tester sends SGd application request message with same session ID in a row and checks the response.
6) The tester sends SGd application request message with different session ID in a row and checks the response.
7) The tester logs in with different user ID and sends SGd application request message with same session ID in step 2 and checks the response.

Expected Results:

1) A confirmation from the tester that the Auth-Session-State AVP is indeed set correctly in response messages.
2) A confirmation from the tester that the neither the Authorization-Lifetime AVP nor the Session-Timeout AVP is present in response messages.
3) In case of a duplicate or non-unique session ID, an error response is generated with Result-Code AVP as DIAMETER_INVALID_AVP_VALUE 5004 and Session-ID AVP is added in Failed AVP.
4) A response message indicating success is received to the request message when session ID is unique.

Expected format of evidence:

A confirmation that the tester has confirmed that:

1. The session ID AVP follows the requirements 1 and 2 in the requirement description.
2. The correct Auth-Session-State, Authorization-Lifetime and Session-Timeout AVP configurations are used.
3. The network product does not accept duplicate session IDs.

Test result (Passed or not)

4.2.7.3 Protecting availability and integrity on Diameter-based SGd interface

Requirement Name: Diameter filtering on the SGd interface

Requirement Reference: TS 29.338 [8], clause 6.3.2.2

Requirement Description:

TS 29.338 [8] defines the following commands and their command codes for the SGd application: MO-Forward-Short-Message-Request (OFR) - 8388645, MO-Forward-Short-Message-Answer (OFA) - 8388645, MT-Forward-Short-Message-Request (TFR) - 8388646, MT-Forward-Short-Message-Answer (TFA) - 8388646, Alert-Service-Centre-Request (ALR) - 8388648 and Alert-Service-Centre-Answer (ALA) - 8388648. It also mentions that the Application ID field for OFR, OFA, TFR, TFA commands allocated by IANA is 16777313 and that for ALR, ALA commands is 16777312.

SMSF provides a mechanism, or rely on the other network function, to filter incoming Diameter messages on the SGd interface based on the Application IDs and command codes.

In particular, SMSF that supports filtering provides a mechanism:

1) To filter incoming Diameter messages on the SGd interface at the Application layer of the stack ISO/OSI.
2) To allow specified actions to be taken when a filter rule matches. In particular at least the following actions should be supported:
   - Discard: the matching message is discarded; no subsequent rules are applied and no answer is sent back.
   - Accept: the matching message is accepted.
   - Account: the matching message is accounted for i.e. a counter for the rule is incremented. This action can be combined with the previous ones. This feature is useful to monitor traffic before its blocking.
3) To enable/disable the logging for each rule for troubleshooting.
4) To filter on the basis of the value(s) of any portion of the protocol header.
5) To reset the accounting.
6) To disable/enable each defined rule.

Threat References: TR 33.926 [4], clause Y.2.2.1, Diameter filtering

Test case:

Test Name: TC_Diameter_SGd_FILTERING

Purpose:

To verify that the Network Product provides filtering for incoming Diameter messages on the SGd interface.

Procedure and execution steps:

Pre-Conditions:

- This test case is applicable only if the network product supports Diameter SGd Interface and the embedded filtering capability
- The tester has the privileges to configure Diameter filtering rules on the network product.
- The vendor declares that Diameter filtering is enabled and provides a list of the filtering rules.
- The vendor includes a guideline to configure the Diameter filtering in the documentation accompanying the network product.
- A network traffic generator or a pcap file containing the Diameter messages is available.
- A network traffic analyser on the network product (e.g. tcpdump) is available.

Execution Steps

1. The tester logs in the network product.
2. The tester configures the network product with the following rules:

a) Accept messages that meet the filtering rules supported by the vendor on the SGd interface.

b) Discard all other messages on the SGd interface.

c) For each rule above the accounting is also enabled.

3. The tester turns on the network traffic analyser on the SGd interface.
4. The tester sends Diameter messages to the network product by replaying a pcap file or using a network generator, ensuring that the messages pass the supported filtering rules.

   a) Using the network analyser, the tester verifies that the messages are correctly received by the network product.

   b) Using the accounting, the tester verifies that the messages are not discarded because response messages are sent back by the network product.
5. The tester sends Diameter messages to the network product by replaying a pcap file or using a network generator, ensuring the messages do not pass the supported filtering rules.

   a) Using the network analyser, the tester verifies that the messages are discarded by the network product.

   b) Using the accounting, the tester verifies that the messages are discarded and that no response is sent back by the network product.

Expected Results:

- For step 4 the tester receives successful Diameter response messages from the network product.
- For step 5 the tester receives no response from the network product.
- For steps 4 and 5, messages that pass and do not pass the filtering rules are correctly accounted.

Expected format of evidence:

A testing report provided by the testing agency which will consist of the following information:

- The used tool(s) name and version information
- Settings and configurations used
- Pcap trace
- Screenshot

Test result (Passed or not)

4.2.7.4 Protecting from unknown peers on Diameter-based SGd interface

Requirement Name: Disabling peer discovery on the SGd interface

Requirement Reference: RFC 6733 [12], clause 5.2;

Requirement Description:

Capability Exchange Request (CER) and Capability Exchange Answer (CEA) are Diameter messages used on SGd interface to discover diameter nodes and know their capability. If peer discovery is enabled, an attacker can connect to the SMSF and learn about its capabilities by sending CER messages. Network products with the SGd interface should be configured to accept only known peers.

To protect SMSF from attacks by unknown peers (attackers), it supports the following requirements:

1) It maintains list of all trusted nodes with static IP addresses in a peer table.
2) It is configured only to respond to the CER messages from trusted nodes listed in the peer table, and it ignores CERs from all other nodes.

Threat References: TR 33.926 [4], Annex Y.2.2.1, Diameter filtering

Test case:

Test Name: TC_DIAMETER_SGd_PEERDISCOVERY

Purpose:

To verify that the SMSF ignores requests from any unauthorized nodes that tries to discover its capabilities.

Procedure and execution steps:

Pre-Conditions:

- This test case is applicable only if the network product supports Diameter SGd Interface.
- The tester has the privileges to configure network product's peer table to include only directly connected peers with static IP addresses.
- The vendor declares that peer discovery is disabled on the network product.

Execution Steps

1) The tester logs in the network product.
2) The tester configures the peer tables of the network product with a list of static IP addresses.
3) The tester configures its source IP using one from the list in the network product's peer table. The tester then sends a CER message by replaying a pcap file or using a network generator:
   a) Using the network analyser, the tester verifies that the message is correctly received by the network product.
   b) The tester verifies that the network product responds with a CEA.
4) The tester configures its source IP to one that is not in the peer table list of the network product. The tester then sends a CER message by replaying a pcap file or using a network generator:
   a) Using the network analyser, the tester verifies that the message is discarded by the network product.
   b) The tester verifies that the network product does not respond with a CEA.

Expected Results:

The network product responds with a CEA for CERs received from the peers listed in its peer table and ignores CERs from all others.

Expected format of evidence:

A testing report provided by the testing agency which will consist of the following information:

- The used tool(s) name and version information
- Settings and configurations used
- Pcap trace
- Screenshot

Test result (Passed or not)

4.2.7.5 Protecting availability and integrity on Map-based SS7 interface

Requirement Name: Map filtering on the SS7 interface

Requirement Reference: TS 33.204 [13], clause 4.1; TS 29.002 [9], clause 12

Requirement Description:

TS 33.204 [13], clause 4.1 mentions "TCAPsec does not validate the TCAP user payload content. Message screening functions for particular message types may be needed on top of TCAPsec." TS 29.002 [9] defines the Short Message Service (SMS) management services in clause 12.

Hence, message filtering mechanism shall be used on Map-based SS7 interface of SMSF to filter and allow only SMS management services related messages which are applicable for SMSF, for example, MAP-MT-FORWARD-SHORT-MESSAGE service, MAP-MO-FORWARD-SHORT-MESSAGE service, and MAP-ALERT-SERVICE-CENTRE service.

In particular, SMSF that supports filtering provides a mechanism:

1) To filter incoming Map messages on the SS7 interface at the Application layer of the stack ISO/OSI.
2) To allow specified actions to be taken when a filter rule matches. In particular at least the following actions should be supported:
   - Discard: the matching message is discarded; no subsequent rules are applied and no answer is sent back.
   - Accept: the matching message is accepted.

Threat References: TR 33.926 [4], clause Y.2.3.1, Map filtering

Test case:

Test Name: TC_Map_SS7_FILTERING

Purpose:

To verify that the Network Product provides filtering for incoming Map messages on the SS7 interface.

Procedure and execution steps:

Pre-Conditions:

- This test case is applicable only if the network product supports Map/SS7 Interface and the embedded filtering capability.
- The vendor declares that Map filtering is enabled and provides a list of the filtering rules.
- The network product is preconfigured with the following rules:
  a) Accept messages that meet the filtering rules supported by the vendor on the SS7 interface.
  b) Discard all other messages on the SS7 interface.
- A network traffic generator or a pcap file containing the Map messages is available.

Execution Steps

1. The tester turns on the network traffic analyser on the SS7 interface.
2. The tester sends Map messages to the network product by replaying a pcap file or using a network generator, ensuring that the messages pass the supported filtering rules.
   a) Using the network analyser, the tester verifies that the messages are correctly received by the network product.
3. The tester sends Map messages to the network product by replaying a pcap file or using a network generator, ensuring the messages do not pass the supported filtering rules.
   a) Using the network analyser, the tester verifies that the messages are discarded by the network product.

Expected Results:

- For step 4 the tester receives successful Map response messages from the network product.
- For step 5 the tester receives no response from the network product.

Expected format of evidence:

A testing report provided by the testing agency which will consist of the following information:

- The used tool(s) name and version information
- Settings and configurations used
- Pcap trace
- Screenshot

Test result (Passed or not)

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

4.3.1 Introduction

There are no SMSF specific additions to clause 4.3.1 of TS 33.117 [2].

4.3.2 Technical Baseline

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

4.3.3 Operating Systems

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

4.3.4 Web Servers

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

4.3.5 Network Devices

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

4.3.6 Network Functions in service-based architecture

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

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

4.4.1 Introduction

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

4.4.2 Port Scanning

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

4.4.3 Vulnerability scanning

There are no SMSF-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 SMSF.

The interface defined for the SMSF are in 4.2.3 of TS 23.501 [6].

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, the following interface and protocols, if supported by the SMSF network product classes in implementation, are in the scope of the testing for SMSF:

- For Nsmsf [7]: the TCP, HTTP2 and JSON protocols.
- For SGd [8]: the TCP/SCTP, Diameter Base and SGd Diameter Application protocol.
- For SS7 [9]: SCTP, M3UA, SCCP, TCAP, Mobile Application Part (MAP) protocol.

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**
2024-09	SA#105	SP-241083				Presented for information and approval	1.0.0
2024-09	SA#105					EditHelp review and upgrade to change control version	19.0.0
2025-07	SA#108	SP-250657	0003	-	F	Clean up of 33.529	19.1.0
2025-07	SA#108	SP-250672	0004	1	F	Solving issues to TS 33.529 according to review conclusion from GSMA NESASG	19.1.0

History

Document history		
V19.1.0	January 2026	Publication