|  |
| --- |
| 3GPP TS 33.529 V0.4.0 (2024-02) |
| Technical Specification.  |
| 3rd Generation Partnership Project;Technical Specification Group Services and System Aspects;Security Assurance Specification (SCAS) for the Short Message Service Function (SMSF) network product class (Release 19) |
|   |
|  |  |
|  |
| The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP.The present document has not been subject to any approval process by the 3GPPOrganizational Partners and shall not be implemented.This Specification is provided for future development work within 3GPPonly. The Organizational Partners accept no liability for any use of this Specification.Specifications and Reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices. |

|  |
| --- |
|  |
| ***3GPP***Postal address3GPP support office address650 Route des Lucioles - Sophia AntipolisValbonne - FRANCETel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16Internethttp://www.3gpp.org |
| ***Copyright Notification***No part may be reproduced except as authorized by written permission.The copyright and the foregoing restriction extend to reproduction in all media.© 2023, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).All rights reserved.UMTS™ is a Trade Mark of ETSI registered for the benefit of its members3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersLTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersGSM® and the GSM logo are registered and owned by the GSM Association |

Contents

Foreword 4

1 Scope 6

2 References 6

3 Definitions of terms, symbols and abbreviations 7

3.1 Terms 7

3.2 Symbols 7

3.3 Abbreviations 7

4 SMSF-specific security requirements and related test cases 7

4.1 Introduction 7

4.2 SMSF-specific security functional requirements and related test cases 7

4.2.1 Introduction 8

4.2.2 Security functional requirements on the SMSF deriving from 3GPP specifications and related test cases 8

4.2.3 Technical Baseline 8

4.2.3.1 Introduction 8

4.2.3.2 Protecting data and information 8

4.2.3.3 Protecting availability and integrity 8

4.2.3.4 Authentication and authorization 8

4.2.3.5 Protecting sessions 8

4.2.3.6 Logging 8

4.2.4 Operating Systems 8

4.2.5 Web Servers 8

4.2.6 Network Devices 8

4.2.7 Security functional requirements on the SMSF– Non Service-Based Interfaces 8

4.2.7.1 Protection on SGd Diameter Interface between SMSF and the Diameter Application Node 8

4.3 SMSF-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 10

4.3.6 Network Functions in service-based architecture 10

4.4 SMSF-specific adaptations of basic vulnerability testing requirements and related test cases 10

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

Editor’s Note: This clause will outline that the present document contains objectives, requirements and test cases that are specific to SMSF network product class.

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”

Editor’s Note: This clause will contain all the references applicable to present document.

# 3 Definitions of terms, symbols and abbreviations

Editor’s Note: This clause will contain all the definitions, symbols and abbreviations applicable to present document.

## 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].

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

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

**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.

## 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 for the assets specific to SMSF as described in TR 33.926 [4].

## 4.2 SMSF-specific security functional requirements and related test cases

Editor’s Note: The clauses will describe the SMSF-specific security requirements and related test cases which were not included in TS 33.117.

### 4.2.1 Introduction

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

Editor’s Note: We will take TS 33.501, TR 33.926, TS 33.117, and TS 23.040 as the starting point, and derive SMSF-specific functional requirements and related test cases.

### 4.2.3 Technical Baseline

Editor's Note: The technical baseline is a set of generic security requirements to be fulfilled by SMSF. The sub clauses and substructures may be modified as per new security requirement clauses.

#### 4.2.3.1 Introduction

#### 4.2.3.2 Protecting data and information

#### 4.2.3.3 Protecting availability and integrity

#### 4.2.3.4 Authentication and authorization

#### 4.2.3.5 Protecting sessions

#### 4.2.3.6 Logging

### 4.2.4 Operating Systems

### 4.2.5 Web Servers

### 4.2.6 Network Devices

### 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 thatprotection of Diameter interface shall be supported according to NDS/IP as specified in 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:* tba

**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 embedded deployments of NDS/IP termination points with SGd Diameter Interface.

**Preconditions:**

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, clause 4.2.3.2.4, excluding execution step 4, and the profiles as mentioned in requirement description shall be followed in pre-conditions.

## 4.3 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

### 4.3.6 Network Functions in service-based architecture

## 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** |
| 2023-11 | SA3#113 | S3-234674 |  |  |  | Skeleton  | 0.1.0 |
| 2023-11 | SA3#113 | S3-235044 |  |  |  | S3-234675, S3-23476, S3-234808 | 0.2.0 |
| 2024-01 | SA3# 114e | S3-240135 |  |  |  | S3-240122 | 0.3.0 |
| 2024-02 | SA3#115 | S3-240874 |  |  |  | S3-240816, S3-240872 | 0.4.0 |