ETSI TS 133 526 V18.1.0 (2024-05)

5G;
Security assurance specification
for the Management Function (MnF)
(3GPP TS 33.526 version 18.1.0 Release 18)

Reference
DTS/TSGS-0333526vi10

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 Web server (https://ipr.etsi.org/).

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™** and **LTE™** 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 under https://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 objectives, requirements and test cases that are specific to the MnF 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 MnF network product class. In the present document, the MnF network product class represents independently deployed management product supporting 3GPP defined management services.

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

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].

MnF Management Function

4 MnF-specific security requirements and related test cases

4.1 Introduction

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

4.2.1 Introduction

The present clause contains MnF-specific security functional adaptations of requirements and related test cases.

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

The requirements and test cases in TS 33.117 [3] clause 4.2.2 apply to the MnF network product class with the following considerations:

- The requirements and test cases in TS 33.117 [3] clause 4.2.2.2 are only applicable when the product supports HTTP/2-based SBI interfaces.

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 MnF-specific additions to clause 4.2.3.2.1 of TS 33.117 [3].

4.2.3.2.2 Protecting data and information – unauthorized viewing

There are no MnF-specific additions to clause 4.2.3.2.2 of TS 33.117 [3].

4.2.3.2.3 Protecting data and information in storage

There are no MnF-specific additions to clause 4.2.3.2.3 of TS 33.117 [3].

4.2.3.2.4 Protecting data and information in transfer

There are no MnF-specific additions to clause 4.2.3.2.4 of TS 33.117 [3].

The test case can also address the MnF-specific threat "Unprotected Management data during transmission" of clause V.2.2.2 in TR 33.926 [2].

4.2.3.2.5 Logging access to personal data

There are no MnF-specific additions to clause 4.2.3.2.5 of TS 33.117 [3].

.

4.2.3.3 Protecting availability and integrity

4.2.3.3.1 System handling during overload situations

There are no MnF-specific additions to clause 4.2.3.3.1 of TS 33.117 [3].

4.2.3.3.2 Boot from intended memory devices only

There are no MnF-specific additions to clause 4.2.3.3.2 of TS 33.117 [3].

4.2.3.3.3 System handling during excessive overload situations

There are no MnF-specific additions to clause 4.2.3.3.3 of TS 33.117 [3].

4.2.3.3.4 System robustness against unexpected input.

There are no MnF-specific additions to clause 4.2.3.3.4 of TS 33.117 [3].

4.2.3.3.5 Network Product software package integrity

There are no MnF-specific additions to clause 4.2.3.3.5 of TS 33.117 [3].

4.2.3.4 Authentication and authorization

4.2.3.4.1 Authentication policy

4.2.3.4.1.1 System functions shall not be used without successful authentication and authorization.

There are no MnF-specific additions to clause 4.2.3.4.1.1 of TS 33.117 [3].

4.2.3.4.1.2 Accounts shall allow unambiguous identification of the user.

There are no MnF-specific additions to clause 4.2.3.4.1.2 of TS 33.117 [3].

4.2.3.4.2 Authentication attributes

4.2.3.4.2.1 Account protection by at least one authentication attribute.

There are no MnF-specific additions to clause 4.2.3.4.2.1 of TS 33.117 [3].

4.2.3.4.2.2 Predefined accounts shall be deleted or disabled.

There are no MnF-specific additions to clause 4.2.3.4.2.2 of TS 33.117 [3].

4.2.3.4.2.3 Predefined or default authentication attributes shall be deleted or disabled.

There are no MnF-specific additions to clause 4.2.3.4.2.3 of TS 33.117 [3].

4.2.3.4.3 Password policy

4.2.3.4.3.1 Password Structure

There are no MnF-specific additions to clause 4.2.3.4.3.1 of TS 33.117 [3]..

4.2.3.4.3.2 Password changes

There are no MnF-specific additions to clause 4.2.3.4.3.2 of TS 33.117 [3].

4.2.3.4.3.3 Protection against brute force and dictionary attacks

There are no MnF-specific additions to clause 4.2.3.4.3.3 of TS 33.117 [3].

4.2.3.4.3.4 Hiding password display

There are no MnF-specific additions to clause 4.2.3.4.3.4 of TS 33.117 [3].

4.2.3.4.4 Specific Authentication use cases

4.2.3.4.4.1 Network Product Management and Maintenance interfaces

There are no MnF-specific additions to clause 4.2.4.4.1 of TS 33.117 [3].

4.2.3.4.5 Policy regarding consecutive failed login attempts

There are no MnF-specific additions to clause 4.2.3.4.5 of TS 33.117 [3].

4.2.3.4.6 Authorization and access control

4.2.3.4.6 Authorization and access control

4.2.3.4.6.1 Authorization policy

There are no MnF-specific additions to clause 4.2.3.4.6.1 of TS 33.117 [3].

The test case can also address the MnF-specific threat "Over-privileged data process" of clause V.2.2.1 in TR 33.926 [2].

4.2.3.4.6.2 Role-based access control

There are no MnF-specific additions to clause 4.2.3.4.6.2 of TS 33.117 [3].

4.2.3.5 Protecting sessions

4.2.3.5.1 Protecting sessions – logout function

There are no MnF-specific additions to clause 4.2.3.5.1 of TS 33.117 [3].

4.2.3.5.2 Protecting sessions – Inactivity timeout

There are no MnF-specific additions to clause 4.2.3.5.2 of TS 33.117 [3].

4.2.3.6 Logging

4.2.3.6.1 Security event logging

There are no MnF-specific additions to clause 4.2.3.6.1 of TS 33.117 [3].

4.2.3.6.2 Log transfer to centralized storage

There are no MnF-specific additions to clause 4.2.3.6.2 of TS 33.117 [3].

4.2.3.6.3 Protection of security event log files

There are no MnF-specific additions to clause 4.2.3.6.3 of TS 33.117 [3].

4.2.4 Operating systems

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

4.2.5 Web servers

4.2.5.1 HTTPS

There are no MnF-specific additions to clause 4.2.5.1 of TS 33.117 [3].

4.2.5.2 Logging

There are no MnF-specific additions to clause 4.2.5.2 of TS 33.117 [3].

4.2.5.3 HTTP User sessions

For the requirement defined in clause 4.2.5.3 of TS 33.117[3]:

- The requirement "In addition to the Session Idle Timeout (see clause 4.2.3.5.2 of TS 33.117 [3]), the Network Product shall automatically terminate sessions after a configurable maximum lifetime. This maximum lifetime defines the maximum session span. When the maximum lifetime expires, the session shall be closed, the session ID shall be deleted and the user shall be forced to (re)authenticate in the web application and to establish a new session. The default value for this maximum lifetime shall be set to 8 hours." may not be applicable to the MnF product.

4.2.5.4 HTTP input validation

There are no MnF-specific additions to clause 4.2.5.4 of TS 33.117 [3].

4.2.6 Network devices

4.2.6.1 Protection of data and information

There are no MnF-specific additions to clause 4.2.6.2.1 of TS 33.117 [3].

4.2.6.2 Protecting availability and integrity

4.2.6.2.1 Packet filtering

There are no MnF-specific additions to clause 4.2.6.2.1 of TS 33.117 [3].

4.2.6.2.2 Interface robustness requirements

There are no MnF-specific additions to clause 4.2.6.2.2 of TS 33.117 [3].

4.2.6.2.3 GTP-C Filtering

The requirement and test case in clause 4.2.6.2.3 of TS 33.117 [3] is not applicable to MnF.

4.2.6.2.4 GTP-U Filtering

The requirement and test case in clause 4.2.6.2.4 of TS 33.117 [3] is not applicable to MnF.

4.3 MnF-specific adaptations of hardening requirements and related test cases.

4.3.1 Introduction

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

4.3.2 Technical Baseline

There are no MnF-specific additions to clause 4.3.2 of TS 33.117 [3].

4.3.3 Operating Systems

4.3.3.1 General operating system requirements and test cases

4.3.3.1.1 IP-Source address spoofing mitigation

There are no MnF-specific additions to clause 4.3.3.1.1 of TS 33.117 [3].

4.3.3.1.2 Minimized kernel network functions

There are no MnF-specific additions to clause 4.3.3.1.2 of TS 33.117 [3].

4.3.3.1.3 No automatic launch of removable media

There are no MnF-specific additions to clause 4.3.3.1.3 of TS 33.117 [3].

4.3.3.1.4 SYN Flood Prevention

There are no MnF-specific additions to clause 4.3.3.1.4 of TS 33.117 [3].

4.3.3.1.5 Protection from buffer overflows

There are no MnF-specific additions to clause 4.3.3.1.5 of TS 33.117 [3].

4.3.3.1.6 External file system mount restrictions

There are no MnF-specific additions to clause 4.3.3.1.6 of TS 33.117 [3].

4.3.4 Web Servers

4.3.4.1 General

There are no MnF-specific additions to clause 4.3.4.1 of TS 33.117 [3].

4.3.4.2 No system privileges for web server

There are no MnF-specific additions to clause 4.3.4.2 of TS 33.117 [3].

4.3.4.3 No unused HTTP methods

There are no MnF-specific additions to clause 4.3.4.3 of TS 33.117 [3].

4.3.4.4 No unused add-ons

There are no MnF-specific additions to clause 4.3.4.4 of TS 33.117 [3].

4.3.4.5 No compiler, interpreter, or shell via CGI or other server-side scripting

There are no MnF-specific additions to clause 4.3.4.5 of TS 33.117 [3].

4.3.4.6 No CGI or other scripting for uploads

There are no MnF-specific additions to clause 4.3.4.6 of TS 33.117 [3].

4.3.4.7 No execution of system commands with SSI

There are no MnF-specific additions to clause 4.3.4.7 of TS 33.117 [3].

4.3.4.8 Access rights for web server configuration

There are no MnF-specific additions to clause 4.3.4.8 of TS 33.117 [3].

4.3.4.9 No default content

There are no MnF-specific additions to clause 4.3.4.9 of TS 33.117 [3].

4.3.4.10 No directory listings

There are no MnF-specific additions to clause 4.3.4.10 of TS 33.117 [3].

4.3.4.11 Web server information in HTTP headers

There are no MnF-specific additions to clause 4.3.4.11 of TS 33.117 [3].

4.3.4.12 Web server information in error pages

There are no MnF-specific additions to clause 4.3.4.12 of TS 33.117 [3].

4.3.4.13 Minimized file type mappings

There are no MnF-specific additions to clause 4.3.4.13 of TS 33.117 [3].

4.3.4.14 Restricted file access

There are no MnF-specific additions to clause 4.3.4.14 of TS 33.117 [3].

4.3.4.15 Execute rights exclusive for CGI/Scripting directory

There are no MnF-specific additions to clause 4.3.4.15 of TS 33.117 [3].

4.3.5 Network Devices

4.3.5.1 Traffic Separation

The requirement and test case in clause 4.3.5.1 of TS 33.117 [3] is not applicable to MnF-specific network product.

4.3.6 Network Functions in service-based architecture

4.3.6.1 Introduction

There are no MnF-specific additions to clause 4.3.6.1 of TS 33.117 [3].

4.3.6.2 No code execution or inclusion of external resources by JSON parsers

The requirement and test case in clause 4.3.6.2 of TS 33.117 [3] is not applicable to MnF-specific network product.

4.3.6.3 Unique key values in IEs

The requirement and test case in clause 4.3.6.3 of TS 33.117 [3] is not applicable to MnF-specific network product.

4.3.6.4 The valid format and range of values for IEs

The requirement and test case in clause 4.3.6.4 of TS 33.117 [3] is not applicable to MnF-specific network product.

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

There are no MnF-specific additions to clause 4.4 of TS 33.117 [3].

Annex A (informative): Change history

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
2023-06	SA#100					Upgrade to change control version	18.0.0
2023-09	SA#101	SP-230902	0001	-	F	Reference correction	18.1.0

History

Document history		
V18.1.0	May 2024	Publication