ETSI TS 133 516 V19.0.0 (2025-10)

TECHNICAL SPECIFICATION

5G;
5G Security Assurance Specification (SCAS)
for the Authentication Server Function (AUSF)
network product class
(3GPP TS 33.516 version 19.0.0 Release 19)

Reference
RTS/TSGS-0333516vj00

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, requirements and test cases that are specific to the AUSF 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 AUSF 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 33.501: "Security architecture and procedures for 5G system".

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

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

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

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 [1] 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 [1].

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].

4 AUSF-specific security requirements and related test cases

4.1 Introduction

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

4.2 AUSF-specific adaptations of 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 AUSF network product class. The proposed security requirements are classified in two groups:

- Security functional requirements derived from TS 33.501 [2] and detailed in clause 4.2.2.
- General security functional requirements which include requirements not already addressed in TS 33.501 [2] but whose support is also important to ensure that AUSF conforms to a common security baseline detailed in clause 4.2.3.

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

The general approach in TS 33.117 [3] clause 4.2.2.1 and all the requirements and test cases in TS 33.117 [3] clause 4.2.2.2 related to SBA/SBI aspect apply to the AUSF network product class.

There are no AUSF-specific test cases according to the security functional requirements on the AUSF deriving from TS 33.501 [2] and security requirements derived from the threats specific to AUSF as described in TR 33.926 [4].

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 AUSF-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 AUSF-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 AUSF-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 AUSF-specific additions to clause 4.2.3.2.4 of TS 33.117 [3].

4.2.3.2.5 Logging access to personal data

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

4.2.3.3 Protecting availability and integrity

There are no AUSF-specific additions to clause 4.2.3.3 of TS 33.117 [3].

4.2.3.4 Authentication and authorization

There are no AUSF-specific additions to clause 4.2.3.4 of TS 33.117 [3].

4.2.3.5 Protecting sessions

There are no AUSF-specific additions to clause 4.2.3.5 of TS 33.117 [3].

4.2.3.6 Logging

There are no AUSF-specific additions to clause 4.2.3.6 of TS 33.117 [3].

4.2.4 Operating Systems

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

4.2.5 Web Servers

There are no AUSF -specific additions to clause 4.2.5 of TS 33.117 [3].

4.2.6 Network Devices

There are no AUSF-specific additions to clause 4.2.6 of TS 33.117 [3].

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

4.3.1 Introduction

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

4.3.2 Technical baseline

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

4.3.3 Operating systems

There are no AUSF-specific additions to clause 4.3.3 of TS 33.117 [3].

4.3.4 Web servers

There are no AUSF-specific additions to clause 4.3.4 of TS 33.117 [3].

4.3.5 Network devices

There are no AUSF-specific additions to clause 4.3.5 of TS 33.117 [3].

4.3.6 Network functions in service-based architecture

There are no AUSF-specific additions to clause 4.3.6 in TS 33.117 [3].

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

4.4.1 Introduction

There are no AUSF specific addtions to clause 4.4.1 of TS 33.117 [3].

4.4.2 Port Scanning

There are no AUSF specific addtions to clause 4.4.2 of TS 33.117 [3].

4.4.3 Vulnerability scanning

There are no AUSF specific addtions to clause 4.4.3 of TS 33.117 [3].

4.4.4 Robustness and fuzz testing

The test cases under clause 4.4.4 of TS 33.117 [3] are applicable to AUSF.

The interface defined for the AUSF are in 4.2.3 of TS 23.501 [5].

According to clause 4.4.4 of TS 33.117 [3], 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 AUSF, the following interfaces and protocols are in the scope of the testing:

- For Nausf: the TCP, HTTP2 and JSON protocols.

NOTE: There could be other interfaces and/or protocols requiring testing under clause 4.4.4 of TS 33.117 [3].

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	0001	-	F	Correction for alignment	16.1.0
2020-12	SA#90e	SP-201004	0002	-	F	Reference of general SBA/SBI aspect in 33.516	16.2.0
2022-03	-	-	-	-	-	Update to Rel-17 version (MCC)	17.0.0
2023-06	SA#100	SP-230677	0005	1	B	Robustness interfaces and protocols defined for AUSF	18.0.0
2023-06	SA#100	SP-230677	0006	-	F	SCAS release reference corrections	18.0.0
2025-10	-	-	-	-	-	Update to Rel-19 version (MCC)	**19.0.0**

History

Document history		
V19.0.0	October 2025	Publication