ETSI TS 133 537 V18.2.0 (2024-05)

TECHNICAL SPECIFICATION

5G;
Security Assurance Specification (SCAS) for the Authentication and Key Management for Applications (AKMA) Anchor Function (AAnF) (3GPP TS 33.537 version 18.2.0 Release 18)

Reference

DTS/TSGS-0333537vi20

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

Important notice

The present document can be downloaded from:
https://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

If you find a security vulnerability in the present document, please report it through our Coordinated Vulnerability Disclosure Program:
https://www.etsi.org/standards/coordinated-vulnerability-disclosure

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

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 requirements and test cases that are specific to the AAnF 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 AAnF 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 TR 33.926: "Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes".

[4] 3GPP TR 33.535: "Authentication and Key Management for Applications (AKMA) based on 3GPP credentials in the 5G System (5GS)".

[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 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].

AAnF	Authentication and Key Management for Applications (AKMA) Anchor Function

4 AAnF-specific security requirements and related test cases

4.1 Introduction

AAnF specific security requirements include both AAnF-specific security functional requirements in relevant specifications as well as security requirements introduced in the present document derived from the threats specific to AAnF as described in TR 33.926 [3].

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

4.2.1 Introduction

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

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

4.2.2.0 General

The general approach in TS 33.117 [2] clause 4.2.2.1 and all the requirements and test cases in TS 33.117 [2] clause 4.2.2.2 related to SBA/SBI aspects apply to the AAnF network product class.

4.2.2.1 AKMA key storage and update

Requirement Name: AKMA key storage update

Requirement Reference: TS 33.535 [4], clause 6.1

Requirement Description: The AAnF stores the latest information sent by the AUSF. After receiving the new generated A-KID and K_{AKMA}, the AAnF deletes the old A-KID and K_{AKMA} and stores the new generated A-KID and K_{AKMA} as specified in TS 33.535 [4], clause 6.1.

Threat References: TR 33.926 [3], Annex W.2.2.3, AKMA key storage and update

Test Case:

Test Name: TC_AKMA_Key_Storage_Update

Purpose:

Verify that the AAnF stores only the latest AKMA context received by the AUSF.

Pre-Conditions:

- Test environment with AUSF and AF. The AUSF and the AF may be simulated.
- AAnF network product is connected in emulated/real network environment.

Execution Steps

Test A:

1) Primary authentication is simulated for a specific UE, leading to the simulated AUSF pushing SUPI, A-KID1, $K_{AKMA}1$ to the AAnF.
2) The AF requests a K_{AF} from the AAnF by proving A-KID1 and AF_ID.

3) Another primary authentication is simulated for the same UE, leading to the simulated AUSF pushing SUPI, A-KID2, K_{AKMA}2 to the AAnF.

4) The AF requests a K_{AF} by providing A-KID1 to the AAnF.

5) The AF requests a K_{AF} by providing A-KID2 to the AAnF.

Expected Results:

The AF received an error message indicating the AKMA context related to A-KID 1 is not found after step 4). After step 5), the AF received a K_{AF} which is different from the K_{AF} that received after step 2).

Expected format of evidence:

Evidence suitable for the interface, e.g., Screenshot containing the operational results.

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 AAnF-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 AAnF -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 AAnF -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

4.2.3.2.4.1 Confidentiality, integrity and replay protections over SBA interface

Requirement Name: Confidentiality, integrity and replay protections over SBA interface

Requirement Reference: TS 33.535 [4], clause 4.4.0

Requirement Description: The SBA interface between the AAnF and the AUSF is confidentiality, integrity and replay protected as specified in TS 33.535 [4], clause 4.4.0

Threat References: TR 33.926 [3], Annex W.2.2.1, Control plane data protection with AUSF

Test Case:

Test Name: TC_PROTECT_SBA_AAnF_AUSF

Purpose:

Verify that the transported data between AAnF and AUSF are confidentiality, integrity and replay protected over SBA interface.

Pre-Conditions:

- AAnF and AUSF network products are connected in simulated/real network environment.

- Network product documentation containing information about supported TLS protocol and certificates is provided by the vendor.
- Tester shall have access to the SBA interface between AAnF and AUSF.

Execution Steps:

The requirement mentioned in this clause is tested in accordance with the procedure mentioned in clause 4.2.2.2.2 of TS 33.117 [2].

Expected Results:

The user data transported between AAnF and AUSF is confidentiality, integrity and replay protected.

Expected format of evidence:

Evidence suitable for the interface, e.g., evidence can be presented in the form of screenshot/screen-capture or pcap traces.

4.2.3.2.4.2 Confidentiality, integrity and replay protections over SBA interface

Requirement Name: Confidentiality, integrity and replay protections over SBA interface

Requirement Reference: TS 33.535 [4], clause 4.4.0

Requirement Description: The SBA interface between AAnF and AF/NEF is confidentiality, integrity and replay protected as specified in TS 33.535 [4], clause 4.4.0

Threat References: TR 33.926 [3], Annex W.2.2.2, Control plane data protection with AF/NEF

Test Case:

Test Name: TC_PROTECT_AAnF_AF_NEF

Purpose:

Verify that the transported data between AAnF and AF/NEF are confidentiality, integrity and replay protected over SBA interface.

Pre-Conditions:

- AAnF and AF/NEF network products are connected in simulated/real network environment.
- Network product documentation containing information about supported TLS protocol and certificates is provided by the vendor.
- Tester shall have access to the SBA interface between AAnF and AF/NEF.

Execution Steps:

The requirement mentioned in this clause is tested in accordance with the procedure mentioned in clause 4.2.2.2.2 of TS 33.117 [2].

Expected Results:

The user data transported between AAnF and AF/NEF is confidentiality, integrity and replay protected.

Expected format of evidence:

Evidence suitable for the interface, e.g., evidence can be presented in the form of screenshot/screen-capture or pcap traces.

4.2.3.2.5 Logging access to personal data

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

4.2.3.4 Authentication and authorization

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

4.2.3.5 Protecting sessions

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

4.2.3.6 Logging

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

4.2.4 Operating systems

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

4.2.5 Web servers

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

4.2.6 Network devices

There are no AAnF-specific additions to clause 4.2.6 of TS 33.117 [2].

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

4.3.1 Introduction

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

4.3.2 Technical Baseline

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

4.3.3 Operating Systems

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

4.3.4 Web Servers

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

4.3.5 Network Devices

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

4.3.6 Network Functions in service-based architecture

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

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

4.4.1 Introduction

There are no AAnF specific addtions to clause 4.4.1 of TS 33.117 [2].

4.4.2 Port scanning

There are no AAnF specific addtions to clause 4.4.2 of TS 33.117 [2].

4.4.3 Vulnerability scanning

There are no AAnF specific addtions 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 AAnF.

The interfaces defined for the AAnF are in 4.2.3 of TS 23.501 [5].

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, for AAnF, the following interface and protocols are in the scope of the testing:

- For Naanf: 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 [2]

Annex A (informative): Change history

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
2023-03	SA#99					Upgrade to change control version	18.0.0
2023-03	SA#99					Correction of the title in a reference	18.0.1
2023-06	SA#100	SP-230677	0002	1	B	Robustness interfaces and protocols defined for AAnF	18.1.0
2023-06	SA#100	SP-230677	0003	1	F	SCAS release reference corrections	18.1.0
2023-09	SA#101	SP-230901	0005	1	F	Editorial corrections to TS 33.537	18.2.0

History

Document history		
V18.2.0	May 2024	Publication