ETSI TS 133 512 V17.3.0 (2022-05)

5G;
5G Security Assurance Specification (SCAS);
Access and Mobility management Function (AMF)
(3GPP TS 33.512 version 17.3.0 Release 17)

Reference
RTS/TSGS-0333512vh30

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:
http://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 http://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

Intellectual Property Rights 2
Legal Notice 2
Modal verbs terminology 2
Foreword 5
1 Scope 7
2 References 7
3 Definitions of terms, symbols and abbreviations 7
3.1 Terms 7
3.2 Symbols 7
3.3 Abbreviations 8
4 AMF-specific security requirements and related test cases 8
4.1 Introduction 8
4.2 AMF-specific adaptations of security functional requirements and related test cases. 8
4.2.1 Introduction 8
4.2.2 Security functional requirements on the AMF deriving from 3GPP specifications and related test cases 8
4.2.2.0 General 8
4.2.2.1 Authentication and key agreement procedure 8
4.2.2.1.1 Synchronization failure handling 8
4.2.2.1.2 RES* verification failure handling 10
4.2.2.1.3 NAS based redirection from 5GS to EPS 12
4.2.2.2 Void 13
4.2.2.3 Security mode command procedure 13
4.2.2.3.1 Replay protection of NAS signalling messages 13
4.2.2.3.2 NAS NULL integrity protection 13
4.2.2.3.3 NAS integrity algorithm selection and use 14
4.2.2.4 Security in intra-RAT mobility 15
4.2.2.4.1 Bidding down prevention in Xn-handover 15
4.2.2.4.2 NAS protection algorithm selection in AMF change 16
4.2.2.5 5G-GUTI allocation 17
4.2.2.5.1 5G-GUTI allocation 17
4.2.2.6 Security in registration procedure 18
4.2.2.6.1 Invalid or unacceptable UE security capabilities handling 18
4.2.2.7 RRCRestablishment in Control Plane CIoT 5GS Optimization 19
4.2.2.8 Security in PDU session establishment procedure 20
4.2.2.8.1 Validation of S-NSSAIs in PDU session establishment request 20
4.2.2.9 Network Slice Specific Authentication and Authorization 21
4.2.2.9.1 NSSAA revocation 21
4.2.3 Technical Baseline 22
4.2.3.1 Introduction 22
4.2.3.2 Protecting data and information 22
4.2.3.2.1 Protecting data and information – general 22
4.2.3.2.2 Protecting data and information – unauthorized viewing 22
4.2.3.2.3 Protecting data and information in storage 22
4.2.3.2.4 Protecting data and information in transfer 22
4.2.3.2.5 Logging access to personal data 22
4.2.3.3 Protecting availability and integrity 22
4.2.3.4 Authentication and authorization 22
4.2.3.5 Protecting sessions 22
4.2.3.6 Logging 22
4.2.4 Operating Systems 22
4.2.5 Web Servers 22
4.2.6 Network Devices 23
4.3 AMF-specific adaptations of hardening requirements and related test cases 23

4.3.1 Introduction....23
4.3.2 Technical baseline....23
4.3.3 Operating systems....23
4.3.4 Web servers....23
4.3.5 Network devices....23
4.3.6 Network functions in service-based architecture....23
4.4 AMF-specific adaptations of basic vulnerability testing requirements and related test cases....23

Annex A (informative): Change history....24

History....25

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 AMF 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 AMF 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 (Release 15): "Security architecture and procedures for 5G system".

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

[4] 3GPP TS 23.003: "Numbering, addressing and identification".

[5] 3GPP TS 24.501: "Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3".

[6] 3GPP TR 33.926: "Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes".

[7] 3GPP TS 33.501: "Security architecture and procedures for 5G system".

[8] 3GPP TS 23.501: "System Architecture for the 5G System".

[9] 3GPP TS 38.413: "NG-RAN; NG Application Protocol (NGAP)".

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 AMF-specific security requirements and related test cases

4.1 Introduction

AMF specific security requirements include both requirements derived from AMF-specific security functional requirements in relevant specifications as well as security requirements introduced in the present document derived from the threats specific to AMF as described in TR 33.926 [6].

4.2 AMF-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 AMF 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 AMF conforms to a common security baseline detailed in clause 4.2.3.

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

4.2.2.0 General

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 AMF network product class.

4.2.2.1 Authentication and key agreement procedure

4.2.2.1.1 Synchronization failure handling

Requirement Name: Synchronization failure handling

Requirement Reference: TS 33.501 [7], clause 6.1.3.3.2

Requirement Description: "Upon receiving an authentication failure message *with synchronisation failure* (AUTS) from the UE, the SEAF sends an Nausf_UEAuthentication_Authenticate Request message with a "*synchronisation failure*

indication" to the AUSF and the AUSF sends an Nudm_UEAuthentication_Get Request message to the UDM/ARPF, together with the following parameters:

- *RAND* sent to the UE in the preceding Authentication Request, and
- *AUTS* received by the SEAF in the response from the UE to that request, as described in clause 6.1.3.2.0 and 6.1.3.3.1.

An SEAF will not react to unsolicited "synchronisation failure indication" messages from the UE.

The SEAF does not send new authentication requests to the UE before having received the response to its Nausf_UEAuthentication_Authenticate Request message with a "*synchronisation failure indication*" from the AUSF (or before it is timed out). "

as specified in TS 33.501[7], clause 6.1.3.3.2.

Threat References: TR 33.926 [6], clause K.2.2.1, Resynchronization

Test Case:

Test Name: TC_SYNC_FAIL_SEAF_AMF

Purpose:

Verify that synchronization failure is correctly handled by the SEAF/AMF.

Pre-Conditions:

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

Execution Steps

Test A:

1) The UE sends an authentication failure message to the SEAF/AMF with *synchronisation failure* (AUTS).
2) The SEAF/AMF sends a Nausf_UEAuthentication_Authenticate Request message with a "*synchronisation failure indication*" to the AUSF.
3) The AUSF sends a Nausf_UEAuthentication_Authenticate Response message to the SEAF/AMF immediately after receiving the request from the SEAF/AMF, to make sure the SEAF/AMF will receive the response before timeout.

Test B:

1) The UE sends an authentication failure message to the SEAF/AMF with *synchronisation failure* (AUTS).
2) The SEAF/AMF sends a Nausf_UEAuthentication_Authenticate Request message with a "*synchronisation failure indication*" to the AUSF.
3) The AUSF does not send a Nausf_UEAuthentication_Authenticate Response message to the SEAF/AMF before timeout.

Expected Results:

Before receiving Nausf_UEAuthentication_Authenticate Response message from the AUSF and before the timer for receiving Nausf_UEAuthentication_Authenticate Response message runs out,

For Test B, the SEAF/AMF does not send any new authentication request to the UE.

For Test A, the SEAF/AMF may initiate new authentication towards the UE.

Expected format of evidence:

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

4.2.2.1.2 RES* verification failure handling

Requirement Name: RES* verification failure handling

Requirement Reference: TS 33.501 [7], clause 6.1.3.2.2

Requirement Description:

"The SEAF shall proceed with step 10 in Figure 6.1.3.2-1 and after receiving the Nausf_UEAuthentication_Authenticate Request message from the AUSF in step 12 in Figure 6.1.3.2-1, proceed as described below:

- If the AUSF has indicated in the Nausf_UEAuthentication_Authenticate Response message to the SEAF that the verification of the RES* was not successful in the AUSF, or
- if the verification of the RES* was not successful in the SEAF,

then the SEAF shall either reject the authentication by sending an Authentication Reject to the UE if the SUCI was used by the UE in the initial NAS message or the SEAF/AMF shall initiate an Identification procedure with the UE if the 5G-GUTI was used by the UE in the initial NAS message to retrieve the SUCI and an additional authentication attempt may be initiated.

Also, if the SEAF does not receive any Nausf_UEAuthentication_Authenticate Request message from the AUSF as expected, then the SEAF shall either reject the authentication to the UE or initiate an Identification procedure with the UE."

As specified in TS 33.501 [7], clause 6.1.3.2.2.

Threat References: TR 33.926 [6], clause K.2.2.3, RES* verification failure

Test Case:

Test Name: TC_RES*_VERIFICATION_FAILURE

Purpose:

1) Verify that the SEAF/AMF correctly handles RES* verification failure detected in the SEAF/AMF or/and in the AUSF, when the SUCI is included in the initial NAS message.
2) Verify that the SEAF/AMF correctly handles RES* verification failure detected in the SEAF/AMF or/and in the AUSF, when the 5G-GUTI is included in the initial NAS message.

Procedure and execution steps:

Pre-Conditions:

Test environment with UE and AUSF. The UE and the AUSF may be simulated.

Execution Steps

A. Test Case 1

1) The UE sends RR with SUCI to the SEAF/AMF under test, to trigger the SEAF/AMF under test to initiate the authentication, i.e. to send Nausf_UEAuthentication_Authenticate Request to the AUSF.
2) The AUSF, after receiving the request from the SEAF/AMF under test, responds with a Nausf_UEAuthentication_Authenticate Response message with an authentication vector to the SEAF/AMF under test.
3) The UE, after receiving the Authentication Request message from the SEAF/AMF under test, returns an incorrect RES* to the SEAF/AMF under test in the NAS Authentication Response message, which will