ETSI TS 133 117 V17.5.0 (2024-04)

Universal Mobile Telecommunications System (UMTS);
LTE;
5G;
Catalogue of general security assurance requirements
(3GPP TS 33.117 version 17.5.0 Release 17)

Reference
RTS/TSGS-0333117vh50

Keywords
5G,LTE,UMTS

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.

1 Scope

The present document contains objectives, requirements and test cases that are deemed applicable, possibly after adaptation, to several network product classes.

Several network product classes share very similar if not identical security requirements for some aspects. Therefore, these are collected in this "catalogue" document applicable to many network product classes. In addition to this catalogue, requirements specific to different network product classes will be captured in separate documents.

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 TR 41.001: "GSM Specification set".

[3] IETF RFC 3871: "Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure".

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

[5] CVE-1999-0511, http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0511

[6] "Practical recommendations for securing Internet-connected Windows NT Systems", https://support2.microsoft.com/default.aspx?scid=kb;%5BLN%5D;164882.

[7] X-Force Vulnerability Report, http://www.iss.net/security_center/static/193.php

[8] IETF RFC 2644: "Changing the Default for Directed Broadcasts in Routers."

[9] 3GPP TS 33.310: "Network Domain Security (NDS); Authentication Framework (AF)".

[10] 3GPP TS 33.501 v15: "Security architecture and procedures for 5G system".

[11] IETF RFC 7540: "Hypertext Transfer Protocol Version 2 (HTTP/2)".

[12] IETF RFC 6749: "OAuth2.0 Authorization Framework".

[13] 3GPP TS 29.501: "Principles and Guidelines for Services Definition".

[14] 3GPP TS 33.501: "Security architecture and procedures for 5G system" (Release 16).

[15] 3GPP TS 33.2:10: "Network Domain Security (NDS); IP network layer security".

[16] 3GPP TS 29.500: "Technical Realization of Service Based Architecture".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions 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].

Machine Accounts: These will be used for authentication and authorization from system to system or between applications on a system and cannot be assigned to a single person or a group of persons.

Personal data: any information relating to an identified or identifiable natural person ('data subject').

Identifiable person: one who can be identified, directly or indirectly, in particular by reference to an identification number, name or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

NOTE: personal data can be gathered from user data and traffic data.

Sensitive data: data that may be used for authentication or may help to identify the user, such as user names, passwords, PINs, cryptographic keys, IMSIs, IMEIs, MSISDNs, or IP addresses of the UE, as well as files of a system that are needed for the functionality such as firmware images, patches, drivers or kernel modules.

System group account: a predefined system account in the network product, usually with special privileges, which has a predefined user id and hence cannot be tied to a single user (individual) in a normal operating environment.

EXAMPLE: the 'root' account.

3.2 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].

API	Application Programming Interface
CIS	Center for Internet Security
JSON	Java Script Object Notation
NF	Network Function
NRF	Network Repository Function
SBA	Service Based Architecture
SBI	Service Based Interfaces
SEPP	Security Edge Protection Proxy
URI	Uniform Resource Identifier
WAS	Web Application Security

4 Catalogue of security requirements and related test cases

4.1 Introduction

4.1.1 Pre-requisites for testing

The SCAS tests, as described in the present specification, are to be applied to a network product whose software and hardware has been brought into use so that the network product can provide the intended functionality, either in a real network environment or in a simulated environment. This implies that, before any testing is performed, the hardware and software has been installed correctly, the network product is powered on, and communication has been established over all standardized interfaces and OAM interfaces related with the network product's functionality, as described in the vendor's documentation.

Communication over external non standardized Interfaces that may exist and are marked as optional, according to the vendor's documentation, shall also be established during testing unless they are explicitly marked as "not recommended" in the vendor's documentation.

For each of the enabled external communication interfaces there may be various optional capabilities. During testing, all such capabilities shall be enabled unless they are explicitly marked as "not recommended" in the vendor's documentation.

In some cases a testcase might require configuration changes as part of the execution steps or pre-conditions. After such test is executed and prior to any further test execution it needs to be ensured that the state of the ToE is restored back in the original state.

SCAS testing is not about security in operations and deployments. So, in particular, SCAS testing is independent of any operator guidelines or considerations on specific deployment scenarios.

4.1.2 Use of tools in testing

The following text shall apply to all test cases described in the present document:

The present document takes into account that the landscape of testing tools evolves more rapidly than SCAS specifications. It is therefore allowed that, for each requirement, the actual test carried out may deviate from the stepwise description of the test case in the present document if the following conditions are fulfilled:

(1) The test is carried out by preferably using Commercial-of-the-Shelf (COTS) and Free-Open-Source-Software (FOSS) tools that are available for other testers that may want to repeat the test. In case a tool not in any of these two categories is used then evidence of the quality assurance of the tool needs to be provided. This applies only to tools used to perform the actual test and not supportive tools needed for setting up the testing environment like for example traffic generators/ simulators.

In cases where a test lab is not able to obtain the necessary tools to perform the test, vendor proprietary test tools may be used by the test lab as long the test tool is controlled under a suitable quality management system (QMS). The test lab ensures that this QMS is in place in order to avail of a vendor’s test tool.

Additionally in cases where the accredited test lab does not have the necessary test environment to perform a test, it shall be possible for the accredited test lab personnel to perform the test in a vendor's test lab. In such cases the accredited lab should record details of test environment, test set-up used and how the test was performed.

(2) The tester provides evidence, e.g. by referring to the documentation of the tool, that the tool is suitable to verify the requirement, and the scope of testing is equal or larger to the one of the test case described in the present document. The evidence needs to be sufficiently detailed for experts in the field of testing, not for the general public.

(3) The tester provides evidence that the tool has been actually used for testing the network product (e.g. by providing a trace).

4.1.3 Documentation Requirements

When a test case makes an assumption on the availability of certain items in the product documentation then this assumption is to be considered part of the requirement even if the requirements text does not mention the documentation.

4.2 Security functional requirements and related test cases

4.2.1 Introduction

The present clause describes the security functional requirements and the corresponding test cases, independent of a specific network product class. In particular the proposed security requirements are classified in two groups:

- Security functional requirements deriving from 3GPP specifications and detailed in clause 4.2.2
- General security functional requirements which include requirements not already addressed in the 3GPP specifications but whose support is also important to ensure a network product conforms to a common security baseline detailed in clause 4.2.3.

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

4.2.2.1 Security functional requirements deriving from 3GPP specifications – general approach

The present clause describes the general approach taken towards security functional requirements deriving from 3GPP specifications and the corresponding test cases, independent of a specific network product class.

It is assumed for the purpose of the present SCAS that a network product conforms to all mandatory security-related provisions in 3GPP specifications pertaining to it, in particular:

- all 3GPP specifications of the 33-series (security specifications) that are pertinent to the network product class;
- other 3GPP specifications that make reference to security specifications or are referred to from one of them.

3GPP has decided to develop test specifications for the UE in the TSs of the 34-series under the responsibility of Working Group RAN5. 3GPP saw, however, no need to develop test specifications for network elements. For network elements, 3GPP rather trusts that tests are run under the responsibility of the vendors.

Security procedures pertaining to a network product are typically embedded in non-security procedures and are hence assumed to be tested together with them.

It is the purpose of the present SCAS to identify security requirements from the EPS and 5G security architecture that require special attention in testing as they may:

(a) lead to vulnerabilities when not satisfied;

(b) not be captured through ordinary testing activity for non-security procedures;

(c) address security-relevant failure cases and exceptions or 'negative' requirements of the kind: "The network product shall not…"

It is not an intention of the present document to provide an exhaustive set of test cases that would be sufficient to demonstrate conformance of all security procedures with the above-mentioned specifications.

4.2.2.2 Security functional requirements derived from 3GPP specifications – general SBA/SBI aspects

4.2.2.2.1 Introduction

The purpose of the sub-clauses in 4.2.2.2 is to identify and describe the general baseline requirements from SBA security architecture and the corresponding test cases. The general baseline requirements are applicable to all Network Function (NF) within the 5G Core (5GC) utilizing Service-Based Interfaces (SBI), independent of a specific network product class.

4.2.2.2.2 Protection at the transport layer

Requirement Name: Protection at the transport layer

Requirement Reference: TS 33.501 [10], clause 5.9.2.1, clause 13.1, clause 13.3.2

Requirement Description:

"NF Service Request and Response procedure shall support mutual authentication between NF consumer and NF producer" as specified in TS 33.501 [10], clause 5.9.2.1;

"All network functions shall support TLS. Network functions shall support both server-side and client-side certificates.

The TLS profile shall follow the profile given in Annex E of TS 33.310 [9] with the restriction that it shall be compliant with the profile given by HTTP/2 as defined in RFC 7540 [11]. "

as specified in TS 33.501 [10], clause 13.1.

"Authentication between network functions within one PLMN shall use one of the following methods:

- If the PLMN uses protection at the transport layer as described in clause 13.1, authentication provided by the transport layer protection solution shall be used for authentication between NFs."

as specified in TS 33.501 [10], clause 13.3.2.

Threat References: TR 33.926 [4], clause 5.3.6.3, Weak cryptographic algorithms

Test case:

Test Name: TC_PROTECT_TRANSPORT_LAYER

Purpose:

Verify that TLS protocol for NF mutual authentication and NF transport layer protection is implemented in the network products based on the profile required.

Procedure and execution steps:

Pre-Conditions:

Network product documentation containing information about supported TLS protocol and certificates is provided by the vendor.

A peer implementing the TLS protocol configured by the vendor shall be available.

The tester shall base the tests on the profile defined by 3GPP in Annex E of TS 33.310 [9] with the restriction that it shall be compliant with the profile given by HTTP/2 as defined in RFC 7540 [11].

Execution Steps

1. The tester shall check that compliance with the TLS profile can be inferred from detailed provisions in the network product documentation.

2. The tester shall establish a secure connection between the network product under test and the peer and verify that all TLS protocol versions and combinations of cryptographic algorithms that are mandated by the TLS profile are supported by the network product under test.

3. The tester shall try to establish a secure connection between the network product under test and the peer and verify that this is not possible when the peer only offers a feature, including protocol version and combination of cryptographic algorithms, that is forbidden by the TLS profile.

Expected Results:

- The network product under test and the peer establish TLS if the TLS profiles used by the peer are compliant with the profile requirements in TS 33.310 [9] Annex E and RFC 7540 [11].
- The network product under test and the peer fail to establish TLS if the TLS profiles used by the peer are forbidden in TS 33.310 [9] Annex E or RFC 7540 [11].

Expected format of evidence:

Provide evidence of the check of the product documentation in plain text. Save the logs and the communication flow in a .pcap file.

4.2.2.2.3 Authorization of NF service access

4.2.2.2.3.1 Authorization token verification failure handling wthin one PLMN

Requirement Name: Authorization token verification failure handling wthin one PLMN

Requirement Reference: TS 33.501 [14], clause 13.4.1.1

Requirement Description:

"13.4.1.1 Service access authorization within the PLMN

2. The NF Service producer shall verify the access token as follows:

   - The NF Service producer ensures the integrity of the access token by verifying the signature using NRF's public key or checking the MAC value using the shared secret. If integrity check is successful, the NF Service producer shall verify the claims in the access token as follows:

   NOTE: Void.

   - It checks that the audience claim in the access token matches its own identity or the type of NF service producer. If a list of NSSAIs or list of NSI IDs is present, the NF service producer shall check that it serves the corresponding slice(s).
   - If an NF Set ID present, the NF Service Producer shall check the NF Set ID in the claim matches its own NF Set ID.
   - If the access token contains "additional scope" information (i.e. allowed resources and allowed actions (service operations) on the resources), it checks that the additional scope matches the requested service operation.
   - If scope is present, it checks that the scope matches the requested service operation.
   - It checks that the access token has not expired by verifying the expiration time in the access token against the current data/time.

3. If the verification is successful, the NF Service producer shall execute the requested service and responds back to the NF Service consumer. Otherwise it shall reply based on Oauth 2.0 error response defined in RFC 6749 [43]. The NF service consumer may store the received token(s). Stored tokens may be re-used for accessing service(s) from producer NF type listed in claims (scope, audience) during their validity time.

Threat References: TR 33.926 [4], clause 6.3.3.1, Incorrect Verification of Access Tokens

Test Case:

Test Name: TC_AUTHORIZATION_TOKEN_VERIFICATION_FAILURE_ONE_PLMN

Purpose:

Verify that the NF service producer does not grant service access if the verification of authorization token from a NF service consumer in the same PLMN fails.

Procedure and execution steps:

Pre-Conditions:

- Test environment with a NF service consumer.
- The NF service consumer may be simulated.
- The network product under test has already mutually authenticated with the NF service consumer.
- The tester shall have access to the interface between the NF service consumer and the network product under test.
- The tester has the NRF's private key or the shared key.
- The network product under test is preconfigured with the NRF's public key or the shared key.

Execution Steps

The network product under test receives the access token sent from the NF service consumer, verifies the access token based on Oauth 2.0.
Test Cases 1~4 are tests on failure handling by the network product under test when the mandatory claims in access token failed verification.

Test Case 1: Verification failure of the access token integrity

1) The tester computes an access token correctly, except that the signature or the MAC is incorrect, e.g., the signature or the MAC is randomly selected, and then includes the access token in the NF Service Request sent from the NF service consumer to the network product under test.
2) The integrity verification of the access token by the network product under test fails.

Test Case 2: Incorrect audience claim in the access token

1) The tester computes an access token correctly, except that the audience claim is incorrect, i.e., the audience claim in the access token does not match the identity or the type of the network product under test, and then includes the access token in the NF Service Request sent from NF service consumer to the network product under test.
2) The network product under test verifies that the integrity of the access token is valid. However, the audience claim in the access token does not match its identity or type.

Test Case 3: Incorrect scope claim in the access token

1) The tester computes an access token correctly, except that the scope is incorrect, i.e., the scope does not match the requested service operation, and then includes the access token in the NF Service Request sent from the NF service consumer to the network product under test.
2) The network product under test verifies that the integrity of the access token and the audience claim are valid. However, the scope does not match the requested service operation.

Test Case 4: Expired access token

1) The tester computes an access token correctly, except that the expiration time has expired against the current data/time, and then includes the access token in the NF Service Request sent from the NF service consumer to the network product under test.
2) The network product under test verifies that the integrity of the access token, the audience and scope claims are all valid. However, the expiration time in the access token has expired against the current data/time.

Test Cases 5~8 are tests on failure handling by the network product under test when the optional claims in access token failed verification.