ETSI TS 133 117 V14.6.0 (2019-10)

Universal Mobile Telecommunications System (UMTS);
LTE;
Catalogue of general security assurance requirements
(3GPP TS 33.117 version 14.6.0 Release 14)

Reference

RTS/TSGS-0333117ve60

Keywords

LTE,SECURITY,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 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

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

Copyright Notification

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is 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 IPR Policy, no investigation, 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.

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

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

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].

CIS Center for Internet 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 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 clasue 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 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.

4.2.3 Technical baseline

4.2.3.1 Introduction

The technical baseline is a generic set of security requirements to be fulfilled by all network products.

In particular these requirements counter the security threats and objectives identified in the TR 33.926 [4] and they basically aim to guarantee the network product confidentiality, integrity and availability.

4.2.3.2 Protecting data and information

4.2.3.2.1 Protecting data and information – general

Adequate security measures for protecting sensitive data shall be implemented as defined in the present document. Further measures (that are beyond the scope of the present document) may be required by local regulation depending on the classification of the data and other factors such as type of network used during transmission, storage location for data, etc.

4.2.3.2.2 Protecting data and information – Confidential System Internal Data

Requirement Name: Unauthorized Viewing

Requirement Description: When the system is not in maintenance mode, there shall be no system function that reveals confidential system internal data in the clear to users and administrators. Such functions could be, for example, local or remote OAM CLI or GUI, logging messages, alarms, configuration file exports etc. Confidential system internal data contains authentication data (i.e. PINs, cryptographic keys, passwords, cookies) as well as system internal data that is not required for systems administration and could be of advantage to attackers (i.e. stack traces in error messages).

Security Objective references: tba.

Test case:

Test Name: TC_CONFIDENTIAL_SYSTEM_INTERNAL_DATA

Purpose:

Verify that no system function reveals sensitive data in the clear

Procedure and execution steps:

Pre-Condition:

The vendor shall provide documentation describing how confidential system internal information that could possibly be revealed in clear-text is handled by system functions.

A list of all system functions in the network product, information on how to enable and execute them should be provided as a part of the vendor's documentation. A system function is every function implemented in the network product needed by the services/functionalities provided by the network product itself.

Execution Steps

Execute the following steps:

1. Review the documentation provided by the vendor describing how confidential system internal information is handled by system functions.
2. The tester checks if all system functions as described in the product documentation (e.g. local or remote OAM CLI or GUI, logging messages, alarms, error messages, configuration file exports, stack traces) whether they reveal any confidential system internal data in the clear (for example, passphrases).

Expected Results:

There should be no confidential system internal data revealed in the clear by each system function.

Expected format of evidence:

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

4.2.3.2.3 Protecting data and information in storage

Requirement Name: Protecting data and information in storage

Requirement Description:

For sensitive data in (persistent or temporary) storage read access rights shall be restricted. Files of a system that are needed for the functionality shall be protected against manipulation.

In addition, the following rules apply for:

- Systems that need access to identification and authentication data in the clear, e.g. in order to perform an authentication. Such systems shall not store this data in the clear, but scramble or encrypt it by implementation-specific means.
- Systems that do not need access to sensitive data (e.g. user passwords) in the clear. Such systems shall hash this sensitive data .
- Stored files on the network product: examples for protection against manipulation are the use of checksum or cryptographic methods.

Security Objective references: tba

Test case:

Test Name: TC_PSW_STOR_SUPPORT

Purpose:

Verify that Password storage use one-way hash algorithm.

Procedure and execution steps:

Pre-Conditions:

- The tester can access the storage of own user account password.
- The tester has privileges to change the password.
- The original password is P1.

Execution Steps

1. The tester accesses the storage where the result of P1 is, and the corresponding hash value is recorded as A
2. The tester changes the password with P2, then the tester record the storage hash value of the new password as B
3. The tester repeats the step 2 to get other records.

4. The tester verifies whether all the records comply with the characteristic of one-way hash result.

Expected Results:

All records comply with the characteristic of one-way hash result.

Expected format of evidence:

Evidence suitable for the interface, e.g. screenshot contains the operation results.

4.2.3.2.4 Protecting data and information in transfer

Requirement Name: tba

Requirement Description:

- Usage of cryptographically protected network protocols is required.
- The transmission of data with a need of protection shall use industry standard network protocols with sufficient security measures and industry accepted algorithms. In particular, a protocol version without known vulnerabilities or a secure alternative shall be used.

Security Objective references: tba

Test case:

Test Name: TC_PROTECT_DATA_INFO_TRANSFER_1

Purpose:

Verify the mechanisms implemented to protect data and information in transfer to and from the Network Product's OAM interface.

NOTE: The test is limited to the OAM interface although the requirement does not have this limitation because the protection of standardised interfaces will be covered by regular interoperability testing and the proprietary use of HTTPS is covered in clause 4.2.5.1.

Procedure and execution steps:

Pre-Conditions:

Network product documentation containing information about supported OAM protocols is provided by the vendor,

A peer implementing the security protocol configured by the vendor (e.g. SSH client supporting SSHv2 or HTTPS client) shall be available.

Network product documentation stating which security protocols for protection of data in transit are implemented and which profiles in TS 33.310 [5] and TS 33.210 [X] are applicable is provided by the vendor.

For TLS, the tester shall base the tests on the profile defined by 3GPP in TS 33.310 [5]. For IKE and IPsec, the tester shall base the tests on the profile defined by 3GPP in TS 33.210 [X]. For protocols, for which 3GPP did not define a security profile, e.g. SSH, the tester shall base the tests on a widely recognised and publicly available security profile.

Execution Steps

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

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

3. The tester shall try to establish a secure connection between the network product 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 security profile.

Expected Results:

The traffic is properly protected, and insecure options are not accepted by the Network Product.

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.

4.2.3.2.5 Logging access to personal data

Requirement Name: Logging access to personal data

Requirement Description:

In some cases access to personal data in clear text might be required. If such access is required, access to this data shall be logged, and the log shall contain who accessed what data without revealing personal data in clear text. When for practical purposes such logging is not available, a coarser grain logging is allowed.

In some cases, the personal data stored in the log files may allow the direct identification of a subscriber. In such cases, the revealed personal information may not expose the subscriber to any kind of privacy violation.

Test case:

Test Name: TC_LOGGING_ACCESS_TO_PERSONAL_DATA

Purpose:

Verify that in cases where a network product presents personal data in clear text that access attempts to such data are logged and the log information includes the user identity that has accessed the data. The test case also verifies that the personal data itself is not included in clear text in the log.

Procedure and execution steps:

Pre-Conditions:

A document which provides a description of where personal data in clear text is accessible on the network product, how it can be accessed, and details of where such access attempts are logged and how to view these logs.

Execution Steps

- The tester verifies that for cases where personal data is accessible in clear text that attempts to access it are recorded in a log, that the log includes the user that has attempted to access the data and that the log does not include the actual personal data in clear-text.
- The tester repeats the check for each case where personal data is accessible.

Expected Results:

All access attempts to personal data (in clear text) are recorded in the described logs, with the user identity included and no personal data is visible in the log.

Expected format of evidence:

Sample copies of the log files.