ETSI TR 133 916 V15.2.0 (2022-01)

Universal Mobile Telecommunications System (UMTS);
LTE;
5G;
Security Assurance Methodology (SECAM)
for 3GPP network products
(3GPP TR 33.916 version 15.2.0 Release 15)

Reference
RTR/TSGS-0333916vf20

Keywords
5G,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 - 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 Report (TR) 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 "**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 Report 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 defines the complete Security Assurance Methodology (SECAM) evaluation process (evaluation, relation to SECAM Accreditation Body, roles, etc.) as well as the components of SECAM that are intended to provide the expected security assurance. It will thus describe the general scheme providing an overview of the entire scheme and explaining how to create and apply the Security Assurance Specifications (SCASs). It will detail the different evaluation tasks (vendor network product development and network product lifecycle management process assessment, Security Compliance Testing, Basic Vulnerability Testing and Enhanced Vulnerability Analysis) and the different actors involved. Enhanced Vulnerability Analysis is outside the scope of the present release of SECAM. The present document will help all involved parties to have a clear understanding of the overall process and the covered threats.

The concrete security requirements will be part of the Security Assurance Specifications (SCASs) for each network product class and not part of this overall process document. Some of the tasks described in the SECAM scheme are meant to be performed by 3GPP, while other tasks are meant to be performed by the SECAM Accreditation Body. This accreditation body has been agreed to be the GSMA. 3GPP maintains the overall responsibility for the SECAM scheme and creates the SCASs. The SECAM Accreditation Body is tasked to develop requirements on vendor network product development, the network product lifecycle management process, and SECAM-accreditation for vendors and test laboratories, and describe these requirements in separate documents that will complement the present document. The SECAM Accreditation Body defines its own scheme that covers all these tasks.

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 33.401: "3GPP System Architecture Evolution (SAE); Security architecture".

[3] void

[4] 3GPP TR 33.821: "Rationale and track of security decisions in Long Term Evolution (LTE) RAN / 3GPP System Architecture Evolution (SAE)".

[5] 3GPP TS 33.102: "3G security; Security architecture".

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

[7] GSMA FS.13: "NESAS Overview v.2.0", https://www.gsma.com/security/resources/fs-13-network-equipment-security-assurance-scheme-overview/

[8] GSMA FS.14: "NESAS Security Test Laboratory Accreditation v.2.0", https://www.gsma.com/security/resources/fs-14-network-equipment-security-assurance-scheme-security-test-laboratory-accreditation/

[9] GSMA FS.15: "NESAS Development and Lifecycle Assessment Methodology v.2.0", https://www.gsma.com/security/resources/fs-15-network-equipment-security-assurance-scheme-vendor-development-and-product-lifecycle-requirements-and-accreditation-process/

[10] GSMA FS.16: "NESAS Development and Lifecycle Security Requirements v.2.0", https://www.gsma.com/security/wp-content/uploads/2021/02/FS.16-NESAS-Development-and-Lifecycle-Security-Requirements-v2.0.pdf

3 Definitions and abbreviations

3.1 Definitions

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

3GPP Security Assurance Methodology (SECAM): SECAM is a process used to measure the security features of 3GPP network products studied and described in the present document.

Accreditation: Formal recognition by an accreditation body that a test laboratory is impartial and competent to carry out specific tests or types of assessments.

NOTE1: In the context of SECAM, it would be recognition that a test laboratory is competent to assess the 3GPP network product against the requirements from the 3GPP SCAS and to produce an evaluation report.

SECAM Accreditation Body: the entity responsible for the accreditation process. This entity is the GSMA.

Assurance: confidence that a network product meets its specific security objectives.

NOTE 2: Assurance is usually verified by performing an evaluation.

Assurance level: evaluation effort in terms of scope, depth and rigor. For higher assurance level, more information with more details is typically required, and this information will be analysed more rigorously.

NOTE 3: The "3GPP Assurance Levels" have nothing to do with "Evaluated Assurance Levels" used in Common Criteria.

Basic Vulnerability Testing (BVT): The process of running security tools against a network product. BVT is defined by the use of Free and Open Source Software (FOSS) and Commercial off-the-shelf (COTS) security testing tools on the external interfaces of the network product.

NOTE 4: Details on these tools can be found in clause 7.2.4.

Certification: confirmation by an independent Certification Authority (CA) that the evaluation has been properly carried out.

NOTE 5: Certification of network products is out of scope for SECAM. However, SECAM does not preclude certification activities for network products which would e.g. complement the Self-declaration step.

Enhanced Vulnerability Testing (EVA): Evaluation process step described in Clause 7.2.5. This activity takes the output of the earlier Security Compliance Testing (SCT) and Basic Vulnerability Testing (BVT) into account.

NOTE 6: Enhanced Vulnerability Analysis is outside the scope of the present release of SECAM.

Evaluation report: the output document delivered by the test laboratory for its evaluation task, in which the test procedures, the test results and other related information may be included. For three specific evaluation tasks defined in SECAM (SCT, BVT, EVA), the according output document is SCT report, BVT report, EVA report respectively.

Test laboratory: enityt that evaluates the network product and produces an evaluation report. The vendor, the operator, GSMA, NVIOT, 3GPP, GCF or some other party, could take the test laboratory role.

Hardening: contributes to the security baseline of a network product, achieved for example by configurations, settings, and protocol restrictions, to decrease the attack surface for a network product. The difference in hardening is one aspect that influences the security baseline of a network product.

Network Product: A network product is the instantiation of one or more network product class(es).

Network Product Class: A network product class, in the context of SECAM, is the class of products that all implements a common set of 3GPP defined functionalities.

Network Equipment Security Assurance Scheme (NESAS): the name given to the scheme that will provide an administrative framework for implementation of SECAM for security evaluation of 3GPP compliant network equipment.

NOTE 7: NESAS is a GSMA term but is not used in this document.

SECAM evaluation: A SECAM evaluation comprises of the Vendor Network Product Development process evaluation, the product lifecycle management process evaluation and the Network Product evaluation.

Security Assurance Specification (SCAS): The SCAS for a given network product class provides a description of the security requirements (which are including test cases) pertaining to that network product class.

Security baseline: The security baseline of an evaluated network product is a set of security requirements and environmental assumptions defining its capacity to resist a given attack potential.

Security Compliance Testing (SCT): Evaluation process step used to describe activities for checking the compliance of a network product with applicable Security Assurance Specifications (SCAS).

Self-declaration: Self-declaration is a declaration of the claims made on the network product by the vendor.
It means that a vendor provides a self-declaration of its network product based on the evaluation report required by SECAM to the operator without any review of a certification authority of these reports before.

Self-evaluation: Self-evaluation is an assessment of the network product by the vendor. It means that the vendor has an accredited evaluation lab in its organization that performs the evaluation of the network product. The evaluation lab assesses the network product against defined criteria and produces an evaluation report according to a formalized and standardized procedure.

Third-party evaluation: Third-party-evaluation is an assessment of the network product by an independent third-party.
It means that a third-party has an accredited evaluation lab that performs the evaluation of the network product.
The evaluation lab assesses the network product against defined criteria and produces an evaluation report according to a formalized and standardized procedure. Third-party evaluation is similar to self-evaluation. The only difference is that the party performing the evaluation is different from the vendor.

Vulnerability: An exploitable issue in a network product rendering it unable to withstand attacks. Vulnerabilities create the risk of successful attacks.

Vulnerability Assessment (VA): The process of assessing the output of SCT or BVT activities to classify the found issues by severity in order to identify those which are relevant vulnerabilities.

3.2 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].

AES	Advanced Encryption Standard
BVT	Basic Vulnerability Testing
CC	Common Criteria
COTS	Commercial Off The Shelf
CPA	Commercial Product Assurance
CVE	Common Vulnerabilities and Exposures
CWE	Common Weakness Enumeration
CVSS	Common Vulnerability Scoring System
EVA	Enhanced Vulnerability Analysis
FASMO	Frequent and Serious Misoperation
FIPS	Federal Information Processing Standard
FIRST	Forum for Incident Response and Security Team
FOSS	Free and Open Source Software
GSF	Generic Security Functionality
GSMA	GSM Association

HW	HardWare
IMEI-SV	IMEI-SoftwareVersion
IT	Information Technology
MME NP	MME Network Product
MME NPC	MME Network Product Class
MME	Mobility Management Entity
MNO	Mobile Network Operator
NB	NodeB
NDPP	Network Device Protection Profile
NESAG	Network Equipment Security Assurance Group
NESAS	Network Equipment Assurance Scheme
NPC	Network Product Class
NPCD	Network Product Class Description
OAM	Operations, Administration and Maintenance
OS	Operating System
OSPP	Operating System Protection Profile
PP	Protection Profile
RAM	Random Access Memory
SCAS	SeCurity Assurance Specification
SCT	Security Compliance Testing
SECAM	Security Assurance Methodology
SFR	Security Functional Requirement
SO	Security Objective
SPD	Security Problem Definition
SR	Security Requirement
SSH	Secure Shell
TCG	Trusted Computing Group
USB	Universal Serial Bus

4 Overview

4.0 Introduction

Security of Network Products should be measurable, comparable, and follow a common standardised baseline. This allows mobile network operators to determine the achieved level of security of network products. 3GPP addresses this by introducing SECAM. SECAM covers:

- creation of security requirements and test specifications – the so-called Security Assurance Specifications (SCAS) – (see Section 4.1) and

- security evaluation of Network Products and evaluation of vendor network product development and network product lifecycle management processes compliance (see Sections 4.2, 4.4, and 4.5).

SECAM is defined in this document.

For trustworthiness of evaluation results and credibility of the entire initiative, security-relevant parts of the vendor network product development and network product lifecycle management processes and the test laboratories should be accredited (see Section 4.2). Accreditation by an external party demonstrates that the actor has the capabilities, skills, and competence to perform their respective tasks.

The SECAM Accreditation Body – currently only the GSM Association (GSMA) – covers accreditation and its governance and maintenance and by that complements this 3GPP activity. The SECAM Accreditation Body defines requirements and processes for:

- vendor network product development and network product lifecycle management processes accreditation [9],

- test laboratory (vendor owned or third party) accreditation [8],

- dispute resolution [7].

- vendor development and lifecycle security requirements [10].

The activities of the GSMA are combined in a single scheme, the **Network Equipment Security Assurance Scheme** (**NESAS**). It is currently being specified in various documents. They are publicly available on the Internet. An overview is provided in the NESAS Overview document [7].

4.1 Scope of a SECAM SCAS

A 3GPP Network Product can have vulnerabilities which, if exploited, can damage the MNO and/or end-users. In order to understand the potential attack vectors which could be used, the first thing to do is to identify the targets of the analysis. Each 3GPP Network Product, is basically a device composed of hardware (e.g. chip, processors, RAM, network cards), software (e.g. operating system, drivers, applications, services, protocols), and interfaces (e.g. console interfaces and O&M interfaces) that allow the 3GPP network product to be managed and configured locally and/or remotely. All these features can expose the 3GPP network product to several potential security attacks. If the network product is securely implemented, managed and configured then some of these attacks can be prevented. The above mentioned security attacks can exploit different 3GPP network product features/ capabilities.

The Security Assurance Specification (SCAS) for a given network product class provides a description of the security requirements and associated test cases pertaining to that network product class. It is assumed that the latest version of the 3GPP Security Assurance documents available at the beginning of a particular instance of an evaluation will be used for 3GPP Security Assurance whatever the 3GPP Release compliance of the other 3GPP functions of the product is. Evaluations performed in the past remain valid, however, even when a new version of the 3GPP Security Assurance documents is published.

As pre-requisite for writing a SCAS, 3GPP defines a complete list of features/capabilities considered to be part of the Network Product Class.

In order to achieve the security assured by a SCAS, the network operator needs to ensure that deployment fulfils the environmental assumptions given in the SCAS. The overall process therefore contains the following steps:

1) 3GPP writes SCAS, which may contain environmental assumptions

2) Accredited security test laboratories (vendors or third party) evaluate network product according to SCAS, but only the single product in a vendor-documented configuration for SECAM testing, without any considerations on the system or network or environment in a specific deployment. Here SECAM stops.

3) when the evaluated network product is being deployed, the operator goes back to the environmental assumptions from the SCAS and tests whether they are fulfilled. This validation of environmental assumptions can only be performed during deployment and is needed for security, but is not part of SECAM, because SECAM is about product-testing.

NOTE 1: Some security requirements might be specific to 3GPP features that only exist from a specific 3GPP Release onwards for a given 3GPP Network Product class. The 3GPP SCAS will give clear indication from which Release onwards the test should be applied. The way to give this indication (by grouping Rel-12 specific tests in an annex or by giving indication in the test case as described in clause 5.2.2.1) is outside of the scope of this Technical Report.

NOTE 2: For features that are standardized in 3GPP specifications, maximum advantage should be taken of existing threat analyses that are available from 3GPP Technical Reports (e.g. TR 33.821 for EPS [4]) or other publications.

4.2 Scope of SECAM evaluation

A SECAM evaluation comprises the Vendor Network Product Development process evaluation, the product lifecycle management process evaluation and the Network Product evaluation

The SECAM evaluation will cover the following tasks:

- Vendor network product development and network product lifecycle management process assurance compliance (assessing if the method used to develop the products is compliant with the Vendor network product development and network product lifecycle management process assurance requirements). Details of this activity can be found in Section 7 and the documents defined by the SECAM Accreditation Body.

- Security Compliance Testing (assessing if requested security requirements are correctly implemented in a network product). This includes Basic Vulnerability Testing (running of a set of FOSS/COTS tools on external interfaces of the Network product).

4.3 Scope of SECAM Accreditation

The actor performing a task should be accredited by the SECAM Accreditation Body for this specific task.

Table 4.3-1: Mapping between SECAM phases and involved party

SECAM tasks	Accredited actor
Generic vendor development and network product lifecycle management process	Auditor appointed by SECAM Accreditation Body
Compliance declaration with the accredited generic vendor development and lifecycle process requirements	Accredited vendor
Security compliance testing	Accredited vendor or accredited third-party test laboratory
Basic Vulnerability Testing	Accredited vendor or accredited third-party test laboratory

Consequently, according to table 4.3-1, SECAM can take different forms, depending on who performs security compliance testing and who performs Basic Vulnerability Testing.
SECAM is intended to enable self-evaluation where the vendors evaluate their network products if they have the proper accreditation for that.

The responsibility for writing and managing the accreditation and monitoring rules is taken by a SECAM Accreditation Body. The SECAM Accreditation Body's role also includes the handling of the dispute resolution process. GSMA takes this role and will provide a clear delineation between SECAM work in 3GPP and in GSMA.

Even if it describes the complete process, including evaluation by accredited actors under SECAM Accreditation Body control and Security Assurance Specifications (SCAS) writing, SECAM does not preclude 3GPP SCAS security requirements and tests cases being used directly by mutual consent between vendors and operators without the accreditation process in place if it so desires. This ensures that the 3GPP SECAM work is not held up by delays in deliverables under the responsibility of external bodies, or by conflicting requirements in different countries (e.g. relating to accreditation).

The presence of a SECAM Accreditation Body as defined above is highly desirable in order to ensure a wide recognition of evaluation results and to have a working dispute resolution process available. Having a SECAM Accreditation Body also avoids the need for each operator to set up a one to one trust relationship with every vendor regarding their testing methods and skills.

Validity of accreditation is defined by the SECAM Accreditation Body.

4.4 Ultimate Output of SECAM Evaluation

The ultimate output of the SECAM evaluation is:

- an evaluation report demonstrating compliance of the network product with the 3GPP security assurance specifications;

- evidence to demonstrate to the test laboratory that the accredited vendor product and development lifecycle processes have been complied with for the network product;

- evidence that the actors performing the evaluation tasks are accredited by the SECAM Accreditation Body.Such evidence is not required if there is consent between operator and vendor to not use the accreditation process, see clause 4.3.

The operator examines the evaluation reports and the evidence that the actors performing the evaluation tasks are accredited by the SECAM Accreditation Body.