ETSI TR 133 916 V14.3.0 (2018-04)

Universal Mobile Telecommunications System (UMTS);
LTE;
Security Assurance Methodology (SCAS)
for 3GPP network products
(3GPP TR 33.916 version 14.3.0 Release 14)

Reference
RTR/TSGS-0333916ve30

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

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.

Foreword

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, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 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: "Network Equipment Security Assurance Scheme – Overview", http://www.gsma.com/NESAS_Overview.

[8] GSMA FS.14: "Network Equipment Security Assurance Scheme – Security Test Laboratory Accreditation Requirements and Process", http://www.gsma.com/NESAS_Test_Lab_Accreditation.

[9] GSMA FS.15: "Network Equipment Security Assurance Scheme – Vendor Development and Product Lifecycle Requirements and Accreditation Process", http://www.gsma.com/NESAS_Product_Lifecycle_Accreditation.

[10] GSMA FS.16: "Network Equipment Security Assurance Scheme – Dispute Resolution Process", http://www.gsma.com/NESAS_Dispute_Resolution.

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.

NOTE6: 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
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 [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.

A pre-requisite for writing a SCAS, 3GPP definesa 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 oft he 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.

4.5 Network product evaluation process

The security assurance process describes how the operator gets assurance regarding the security of the network product. The process is depicted in figure 4.5-1. If there are any regulatory requirements on security assurance of the network

product, they will for the purpose of this process model be considered being included in the acceptance requirements of the operator.

When a vendor is ready to provide security assurance w.r.t. a given network product, the vendor obtains one or more Security Assurance Specifications (SCASs) that the network product is aiming to fulfil. Choice of which SCASs to select may depend on operator and/or regulatory input. Then the product is evaluated against the Security Assurance Specification(s). The evaluation results in an evaluation report.

Once the operator received the evaluation report, the operator then decides if the results are sufficient according to its internal policies and whether to accept the security assurance level of the network product or not. The operator's acceptance decision may depend on external forces such as regulatory requirements.

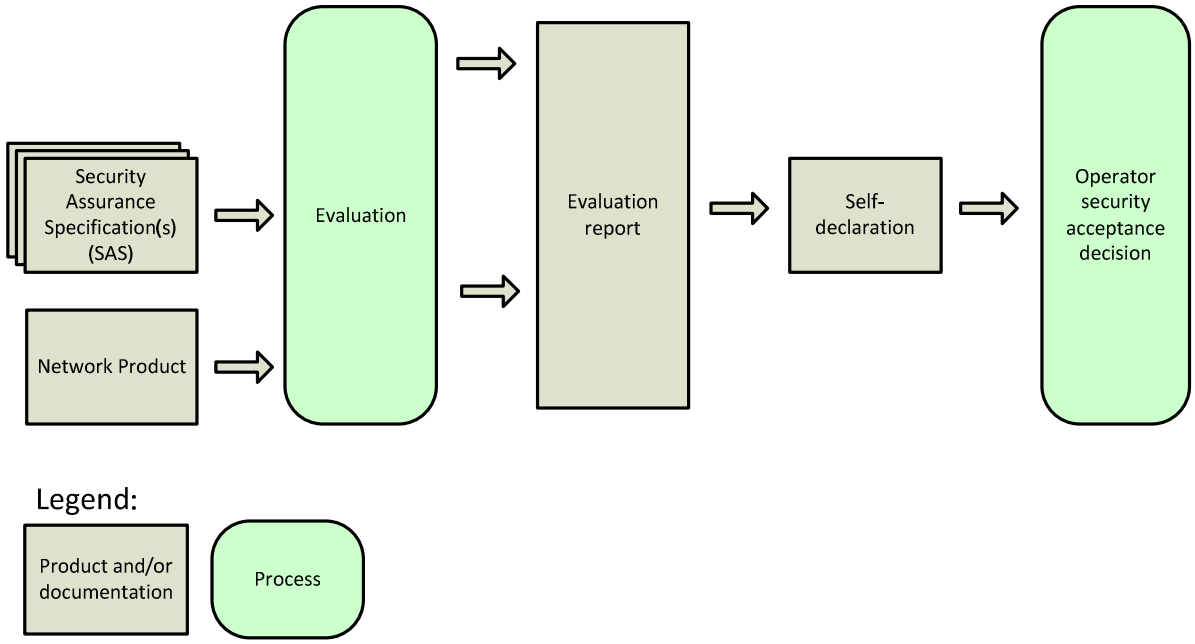

Figure 4.5-1: SECAM defined Security assurance process

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 (cf. clause 7.3).

The SECAM security assurance process is described in depth in clause 7.

4.6 Roles in SECAM

4.6.1 SECAM Roles Overview

The basic roles are implicit from the existing business environment. These roles are the following:

- **Vendor** produces the network product.
- **Test laboratory** is a **Test Laboratory** (accredited third-party test laboratory or accredited vendor test laboratory) that evaluates the network product, evaluates evidence of compliance to the vendor developmenent and product lifecycel requirements, and produces an evaluation report.
- **Operator** makes the decision regarding accepting assurance of security properties of the product for that vendor.
- **3GPP** is responsible for producing Security Assurance Specifications (SCASs).
- **SECAM Accreditation Body** is responsible for accreditation tasks as applicable. This role is assumed by **GSMA.**

4.6.2 Examples of instantiation of roles in SECAM

4.6.2.1 Introduction

The following subclause contains an example for instantiation of roles in SECAM.

4.6.2.2 Example: Complete self-evaluation

Complete self-evaluation of a 3GPP network product (e.g. eNodeB B from vendor Y)

This second example below is similar to the first one except that the vendor conducts all the phases of evaluation.

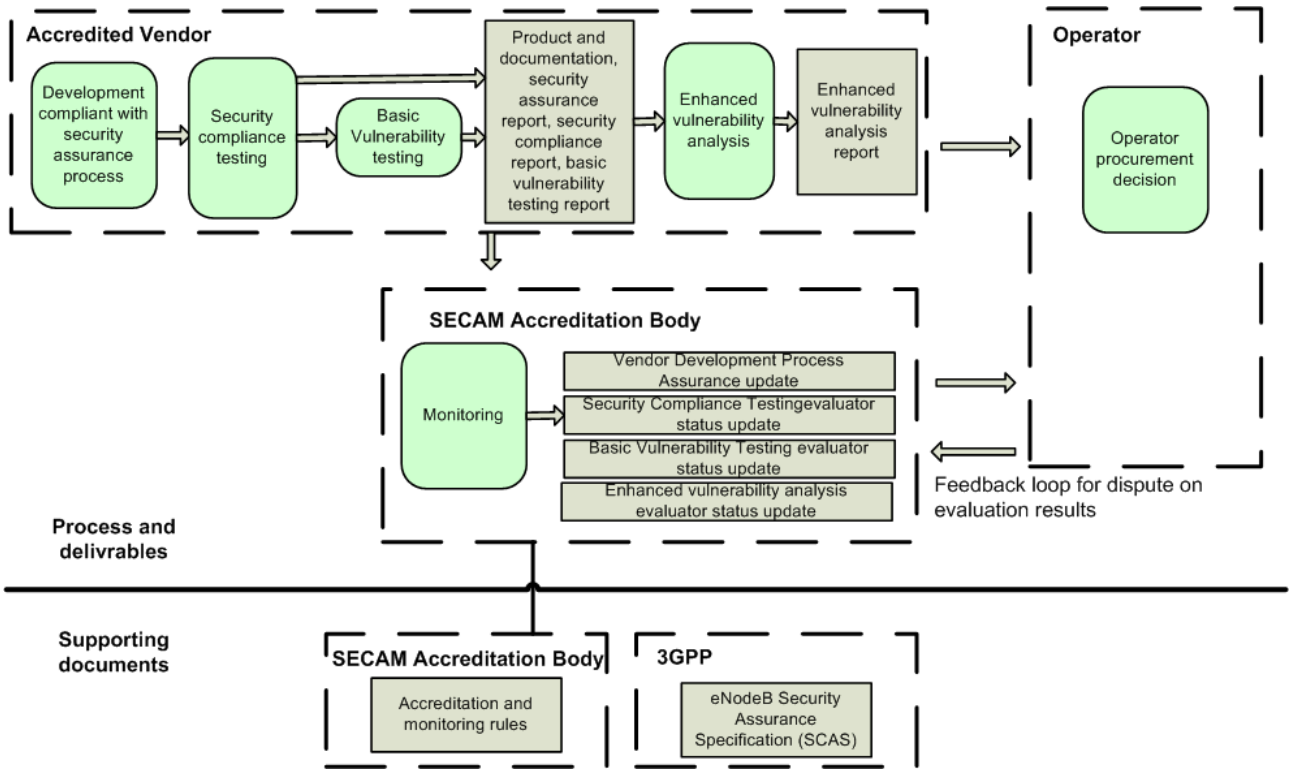

Figure 4.6.2.2-1: Complete self-evaluation of a 3GPP network product (e.g. eNodeB B from vendor Y)

Evaluation results check by the operators and dispute.

4.7 Operator security acceptance decision

The operator examines the network product, the security compliance testing, including the basic vulnerability testing analysis reports, the self-declaration as well as the optional evidence of accreditation from the SECAM Accreditation Body for the actors performing the evaluation task and decides if the results are sufficient according to its internal policies. In particular, the operator can perform a sample of the security compliance testing and basic vulnerability testing, based on the delivered test procedures.

The vendors and third-party laboratories accreditation documents monitored and maintained by the SECAM Accreditation Body attest the trustworthiness of these actors and can help operators in their security acceptance decisions.

The operator does not need to be accredited to perform again the tests made by the test laboratories in order to gain a higher level of assurance that the SECAM evaluation provided trustable results. Definition of the tools and methods for these supplementary evaluations is outside of the scope of SECAM and left as operators' proprietary procedures.

However, in case of disagreement on the test results and if the operator wants to enter a conflict resolution process with the SECAM Accreditation Body and the vendor, some forms of recognition of the validity of the operator's complaint might be useful. This description will be part of the description of the complete dispute resolution process. It is left to the SECAM Accreditation Body and is outside the scope of 3GPP.

4.8 SECAM Assurance level

Assurance level is related to evaluation effort in terms of:

- scope – that is, the effort is greater when a larger portion of the IT product is evaluated; For example, when supplementary aspects of the functionality are included in the evaluation;

- depth – that is, the effort is greater when evaluation is deployed to a finer level of design and implementation detail;

- rigour – that is, the effort is greater when evaluation is applied in a more structured, formal manner. For example, for a given security requirement to test, the effort is greater if the test laboratory is requested to provide a formal demonstration that the product will always behave as intended versus providing a given set of output test data for a limited set of test cases.

In SECAM:

- Scope is constant: SECAM provides a single process for a given network product class, which will be relevant to this class.

- Depth of evaluation is also considered to be constant. The paradigm of SECAM consists in:

    - Security compliance testing: the paradigm would consist in black box verification of security requirements, but exceptions would be possible, e.g.:

        - when required in order to demonstrate compliance for requirements on cryptography, key storage, secure deletion, or implementation of protocols, etc. (in such cases, code inspection would be more efficient than a functional test);

        - when a white/grey box approach is considered more efficient (a black box vulnerability scan over the network would take longer and reveal less than a white box local system analysis).

    - Vulnerability testing: the general paradigm of vulnerability testing would be consistent with the expected attacker model. Such testing will consequently be based on black box vulnerability testing unless the expected attacker is considered having a higher potential. In the latter case, white/grey box penetration testing would be necessary to assess the resistance of the network product. For example, if an attacker were believed to have knowledge of the implementation of the network product, a black box assessment only would be unreasonable.

    - Build process assurance: Verification of build process is limited to basic functional documentation, use of a configuration system and providing of operational guidance.

- Rigour of verification is also considered constant, since it focuses on demonstration for functional testing and vulnerability assessment, justification when necessary, and does not require formal demonstration.

Considering that the three parameters are expected to be constant and the above mentioned additional complexity of having several assurance levels, SECAM considers only one assurance level per network product class. However it is expected that different product class are confronted by different attacker models, and have consequently to undergo different levels of rigour or depth of evaluation.

SECAM consequently considers only one assurance level per network product class.

4.9 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.

This resistance to a given attack potential relies on:

- Attacker model and attacker potential agreed to be relevant for a given network product class.

- The completeness and correct implementation of security requirements and operational environment assumptions which limit the capacity of this attacker to threaten given assets:

    - Security requirements can be more demanding in some network elements, e.g. exposed nodes will have to implement hardening requirements which will not necessarily be needed in elements less exposed.

    - Vulnerability assessment will be performed with more depth whenever the element is expected to resist a stronger attacker.

It is necessary to state in a well-defined way in which environment the 3GPP-defined functionality is assumed to be operating and what types of attackers (if any) may be able to launch attacks from the outside as well as from the inside of this environment. This assessment is accomplished during the SCAS writing phase and be related to the threat and risk analysis outcomes.

At the end of this process, for each network product class, 3GPP will have precisely defined the attacker model as well as the operational environment assumption and the security requirements to mitigate the identified risks.
The modularity of SCAS allows an easy composition of SCAS modules to describe all the countermeasures of a given network product class and to take the particular environment of the node into account.

The entire set of security requirements, operational environment assumptions and attacker model is built to achieve a security baseline deemed relevant by 3GPP for a network product class. This results in one security level per network product class (security baseline MME, security baseline HSS, security baseline eNodeB, etc.).
These baselines are not meant to be compared to one another as they apply to different network product classes.

NOTE: Alternatively, but in rare cases, if no satisfactory average can be found, SECAM could define a new network product class: e.g. collapsed RNC/NBs could be a class different from classical RNCs.

SECAM consequently considers only one security baseline per network product class.

5 Security Assurance Specification (SCAS) Creation

5.1 Writing process overview

An SCAS document will be defined for a specific network product class within the normative phase. On a high level, the process of writing SCAS documents for a given network product class follows these steps:

- **Describe and model the network product class**
  The network product class is described and modelled to a sufficiently detailed level so as to ensure that the security requirements can clearly describe what data and functions are intended to be protected and which functionalities are required. This modelling will be used as an input document for the following Security Problem Definition.

- **Define the security problem**
  By identifying which assets in the model of the network product class require protection and how these assets can be exploited by an attacker. The security problem definition also contains the security objectives of the network product class under analysis (i.e. which assets require what type of protection), and defines an attacker potential the network product class is supposed to resist. This step also contains the threat analysis employed to understand how an attacker performing the identified potential attacks may misuse the identified assets of the network product class. This provides a concrete security problem that is to be solved, which allows the selection of security requirements that are necessary and sufficient to solve the identified security problem. This material will be contained in a 3GPP Technical Report of the 900-series.

- **Identify the security requirements and test cases**
  Security requirements are derived from the security problem definition. The fulfilment of these requirements ensures that the security objectives can be reached. Catalogues of security requirements and security requirement categories that have been used by operators in practice will be used as a starting point to help 3GPP in writing complete requirements.
  These requirements can and will be modified and adapted as seen necessary by 3GPP.

  In addition, if requirements, or terminology used to specify the requirements, are not clear or consistent there is an increased risk of different understanding of the requirements and this may unnecessarily result in heavy use of the dispute resolution process. For example if a requirement applies on the "management traffic", a clear definition on what the "management traffic" consist of would be needed. This could be in particular a difficulty for tests that consist of verifying whether a requirement is fulfilled by examining documentation and making a decision on whether the designed mechanism or used process fulfils the requirement; such tests are a judgment call and can be called differently by different parties.

The consistency of the requirements format is ensured by the template for a security requirement described in clause 5.2.3.3.

For each security requirement 3GPP will define a test case.

- **Verify the Security Requirements**
  Once the security requirements have been identified it is verified that the security objectives are met by these security requirements, and that every security requirement contributes to defending an identified security objective. If any mismatch is found (e.g. security objective not covered with the existing security requirements or security requirements which do not resolve any security objectives), the list of security requirements is updated accordingly by removing or adding security requirements.

5.2 SCAS documents structure and content

5.2.1 General

According to clause 5.1, the SCAS documents contain three parts, a Network Product Class Description, a Security Problem Definition and the Security Requirements (including the test cases) for any specific Network Product Class [see clause 3.1], to counteract the risks outlined by the threat analysis. Consequently SCAS documents contain the following parts:

- ***Network Product Class Description (NPCD):*** This clause includes the description of the network product class, e.g. the physical and logical interfaces the product class supports to interact with external entities and the major functionalities of the NPC. This material will be contained in a 3GPP Technical Report of the 900-series.
- ***Security Problem Definition (SPD):*** This clause defines the security problem that is to be addressed and the security objectives of the network product class. This material will be contained in one or more 3GPP Technical Reports of the 900-series.
- ***Security Requirements (SR):*** This clause defines the security requirements, which may include hardening requirements, selected according to the Security Problem Definition and the requirements strictly related to the 3GPP features implemented by the network product class under analysis. Requirements and test cases will be contained in one or more 3GPP Technical Specifications.

In the following a detailed description of the SCAS parts SPD and SR is provided.

5.2.2 Security Problem Definition (SPD)

5.2.2.1 Introduction

For the Security Problem Definition (SPD) part of the SCAS writing phase, the steps to be accomplished by 3GPP for a given network product class are:

- List the critical assets of the network product class.
- List the assumptions on the Operational Environment
- Identify the attacker model for the Network Product Class.
- Identify threats, i.e. adverse actions than can be performed on assets.
- Identify the threat relevance (Mitigate, Accept, and Transfer).
- Identify the level (probability and impact) of risk associated with the threats and assess a risk by comparing the risk level with the cost for mitigation.

NOTE 1: This risk assessment will have to be provided in general only when the threat relevance is challenged by someone.

- Identify the list of the security objectives necessary to face the identified threats and reduce the risk surface.

For features that are standardized in 3GPP specifications some threat analyses are available from e.g. TR 33.821 for EPS [4] or other publications. In particular, threat analyses related to the security requirements in 3GPP TSs to be re-

used in SCAS, see clause 5.2.3.2, need not be repeated in SCAS. These were however written before e.g. current SCAS type of work objectives came to light.

NOTE 2: For features that are (to some degree) proprietary and, hence, not (fully) standardized, a way of describing them in a general way needs to be found as, by their nature, no common understanding is generally available to the public. Without a general description of a feature, it may be difficult to perform a threat and risk analysis on it.

NOTE 3 To ensure consistency across threats and security objectives the following set of guidelines should be applied when analysing proposed threat and security objectives.

- Threat descriptions should avoid including security objectives or requirements or countermeasure implementation details.
- Check if there is an existing threat in a 3GPP TR of the 900-series before attempting to create a new one. For example a variant of an existing threat could be created.
- Attempt to map the threat to one of the existing threat categories before creating a new threat category.
- Details in the threat description should indicate if the threat is a high level threat (refers to several attack components) or a detailed threat (refers to a specific attack component).
- Attempt to map the threat to one of the existing security objectives before creating a new security objective.
- All requirements should map to one or more threats.
- All requirements should map to one or more security objectives.
- It should be clear from the text in the requirement description field that the requirement is a detailed specific requirement (which has its own test case(s)) or is a high level requirement (e.g. conformance to industry best practices) which has multiple test cases.
- A new threat, threat category, or security objective should be included only after 3GPP determined that sufficient rationale was provided.

5.2.2.2 Threats

There are many threat and risks analysis or modelling frameworks available for IT equipment and computers networks. None of them provided a perfect fit the needs of SECAM whose ultimate goal is to be capable to derive concrete and testable security requirements to reduce the level of exposure of telecom equipment.

This process is likely to be iterative and there will be some trade-off in terms of time. It is not a goal to be absolutely complete in the threats assessment. What ultimately matters in the threat analysis phase is that 3GPP determines that the achieved level of details is good enough to be able to easily derive testable security requirements to cover the risks in a reasonable amount of time.

The structure for a threat description is provided here to indicate the information needed for having a clear security problem definition. This can help to facilitate the identification of the security requirements. Hereafter a possible structure for the threats, risks and security objectives which are part of the SPD is reported. This structure will be related to the threat modelling framework used for the analysis and consequently this proposal could be changed accordingly:

- *Threat Name:* each threat is assigned a unique name. The name preferably indicates the topics covered by the threat.
- *Threat Reference*: a unique short form is assigned to each threat as a primary means for referencing the threat. The convention adopted is: <threat category> - <progressive number> where the convention adopted for the "threat category" can be the first two letters of the category to which the threat belongs or similar.-

  Threat Category: a reference to the category to which the threat belong based on the classification (threat methodology) that will be adopted.
- *Threatened Asset:* an indication of the network product assets that are object of the threat.

- *Threat Description*: the adverse actions that can be performed by a threat agent on an asset. These actions influence one or more properties of the asset from which that asset derives its value. Examples of threat agents are hackers, users, computer processes, and accidents. Threat agents, and their level, may be further described by aspects such as expertise, resources, opportunity and motivation. To provide a basis for requirements that are on roughly the same level, 3GPP chooses a level of threat agents that the system should be able to withstand (although the levels may be hard to quantify or measure). Protection mechanisms or requirements then are not selected if a threat can be instantiated only by a threat agent of higher level. This is in line with the single assurance level and single security baseline per network product class of clause 4.

- *Threat relevance:* the threat relevance (Mitigate, Accept, and Transfer).

Further details are given in 33.926 [6].

5.2.2.3 Security Objectives

The Security Objectives countering the defined threats are likely to overlap in many cases. Therefore, they are to be listed in a separate section of the SCAS document to aggregate references to the threats they counter.

The structure for Security Objective is as follows:

- *Security Objective Reference:* a unique short form is assigned to each Security Objective as a primary means for referencing. The convention adopted is: SO - <progressive number>-

- *Security Objective:* the concise and abstract statement as given for the threats.

- *Threat References:* List of Threat References of the threats countered by the Security Objective in question.

Additionally, a table matching the Threats and Security Objectives should be given in an annex TR 33.926 [6].

5.2.3 Security Requirements

5.2.3.1 Introduction

3GPP will have to list the countermeasures deemed relevant to mitigate the risks identified in the threat assessment. These countermeasures will take the form of either:

- security requirements on the network product with associated test cases; or

- operational environment security assumptions for a given product class.

The Security Requirements clauses within the the pertinent 3GPP TS contain the security requirements identified according to the threats (see figure 5.2.3.1-1).

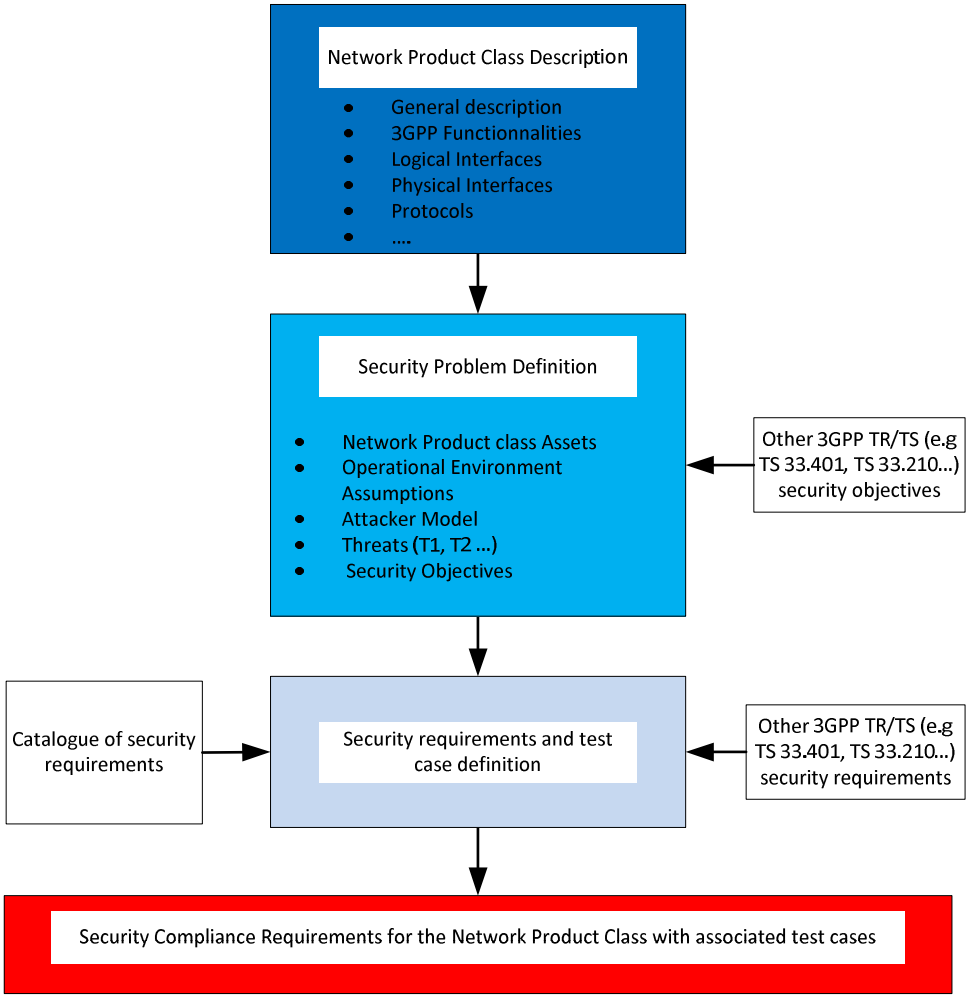

Figure 5.2.3.1-1: Process for deriving security requirements in a SCAS document

The security requirements will include security functional requirements as well as hardening requirements and basic vulnerability testing requirements. The security functional requirements are ensuring the existence of security functionalities in the network products in order to achieve security objectives (e.g. 3GPP functional requirements). The hardening requirements are either ensuring the absence of unneeded or insecure functionality, or impose a restriction on a function forcing it to behave in a more secure way. The basic vulnerability testing requirements specify the areas to be subjected to basic vulnerability testing.

The purpose of hardening is to reduce the attack surface and security vulnerability of the network product and to ensure that security functions of the network product cannot be bypassed. SECAM will specify hardening requirements that should be part of the evaluation. Those requirements are only intended to reduce the attack surface rather than directly related to a security function. All security requirements, those related to a specific security function as well as those related to the reduction of the attack surface and basic vulnerability testing requirements, will be treated on the same footing and the text of clause 5.2.3.3 applies to all "types" of requirements. Their evaluation will be based on the tests cases of the SCAS. In any case, hardening requirements imply that they are implemented before evaluation through test cases. Hardening requirements should be formulated generic enough, or in different variants, to be applicable for a variety of anticipated operating systems and applications. Hardening is needed to let network products achieve the given security baseline and assurance level, alongside with other security requirements.

Hardening can be the removal of services, protocols, ports, etc. in order to reduce known security vulnerabilities and minimize the risk in an existing but unneeded functionality. An example of hardening is to remove unnecessary services of general purpose software used in a specific context. It can also be a physical action like removing unneeded USB ports. An example of such a requirement is provided at the end of clause 5.2.3.3.

SECAM security requirements represent the common agreement of operators and vendors on what has to be implemented for a given network product class to achieve the required security baseline. All those requirements (including operator's initialization and configuration requirements which have been channelled through the relevant SECAM standardization processes) have to be taken into account from the beginning of the development and design

phase of the network product as well as in subsequent updates of the network product. This will ensure that network products will be developed in a way that:

a) Maximizes their likelihood to pass SECAM evaluation.

b) They operate correctly and securely when deployed in operator's networks.

c) Avoids costly patching cycle to ensure a) and b).

5.2.3.1.1 Level of detail of security requirements

Security requirements can be specified in different levels of detail, with a tradeoff between precision of the requirement and its general applicability.

Detail Level 1: Security requirements of general system-independent nature: What needs to be secured?

Example: data storage in general

Detail Level 2: Security requirements that are system-specific but still product-independent: What needs to be secured, for this system type?

Example: data storage in databases

Detail Level 3: Product-specific security requirements: How does this specific product need to be secured?

Example: data storage in an Oracle database Vx.y

In order to ensure consistency between all requirements in a SCAS, every requirement of detail level 2 or 3 should be derived from a generic level 1 requirement or security objective.

In general, requirements on detail level 3 should be avoided in a SCAS because that would limit direct applicability of a SCAS for some network products.

5.2.3.2 Incorporation of security requirements from existing 3GPP TSs in current releases

In figure 5.2.3.1-1, 3GPP specifications represent an input for both SPD and security requirements definition, where the latter includes test case definition. The reason for this assumption is that 3GPP security specifications (e.g. TS 33.401 [2]) already contain several security objectives and related security functional requirements which 3GPP identified when designing UMTS and LTE. When looking at such type of security functional requirements, they can be grouped into three categories:

1) Security functional requirements related to protocols and behaviours necessary for secure interoperability between nodes from different vendors that require a certain positive behaviour of a 3GPP function.
For example, the security functional requirement " The MME sends to the USIM via ME the random challenge RAND and an authentication token AUTN for network authentication from the selected authentication vector. " retrieved from TS 33.401 [2], belongs to this category.

2) Security functional requirements related to protocols and behaviours necessary for secure interoperability between nodes from different vendors that require that a 3GPP function does not perform a certain action.
For example, the security functional requirement " Access to E-UTRAN with a 2G SIM or a SIM application on a UICC shall not be granted " retrieved from TS 33.401 [2] belongs to this category.

3) Security functional requirements not related to protocols or behaviours necessary for secure interoperability between nodes from different vendors, but rather deal with security features which are supported by the network products and consequently strictly related to their implementation.
For example, the security functional requirements specified in clause 5.3 of TS 33.401 [2] for eNBs and in annex I of TS 33.102 [5] for RNCs in exposed locations belong to this category.

The security functional requirements in the first group are already covered by the interoperability and conformance testing and SECAM documents do not repeat these requirements or add tests for them.

The security functional requirements in the second category may not be covered by the interoperability and conformance testing. In this case a SCAS document may contain a reference to these requirements with the related test

cases which verify that the network products adhere to the security functional requirements. As an example, security functional requirements for the MME in the second category are collected in TS 33.116.

The security functional requirements in the third category are within the scope of SECAM and they will be taken into account by the security requirements for the compliance testing. However, for some network product classes, e.g. the MME, there are no requirements in the third category.

A security compliance requirement in a SCAS that references a 3GPP TS refers to the corresponding TS security functional requirement and also contains a test description how to verify the correct implementation of the described security functional requirements.

SECAM does not provide stand-alone security assurance requirements. Instead, SECAM provides a test case for every security requirement.

5.2.3.3 Handling of security requirements

A SECAM Catalogue of General Security Assurance Requirements and associated test cases is providedbecause several network product classes will share very similar if not identical security requirements for some aspects. This catalogue therefore allows to maximize the reuse of already written requirements. This approach matches the requirement that a SCAS will have to be developed in a modular fashion such that an individual module is generic enough to be applied to more than one network product class. This approach can help to prevent from writing the same security requirements from scratch several times in different network product class SCAS (see clause 4 of the present document).

It is important to underline that the 3GPP catalogue is constructed while working on SCASs for specific network product classes, and the intention is not to first create the catalogue in an abstract way and then write the first SCAS based on it. No requirements is included in the catalogue before it has been found useful for a specific network product class. This prevents the catalogue from accumulating "good-to-have" requirements that are never used specific network product classes. Consequently, the way to build the proposed catalogue is an iterative process that counts the following steps:

1) Start the normative phase for a specific Network Product Class (e.g. MME).

2) Select from the identified sources the proper security requirements that meet the needs of the security objectives and adapt them to SECAM.

3) Add this adapted requirements in the SECAM catalogue in order to reuse if possible during the normative phase of other Network Product Classes.

4) Start the normative phase of another Network Product Class (e.g. eNB) and refer to the security requirements already available in the SECAM catalogue if possible otherwise select the new ones from the agreed sources and update the Catalogue.

Security requirements are expected to follow a template similar to the one described hereafter:

Template for a Security Requirement Description

Statements of security requirements are intended to be clear, concise and unambiguous. In particular, each security requirement includes:

- *Requirement name*: each security requirement is assigned a unique name. The name indicates the topics covered by the requirement:

- *Requirement reference:* a unique short form of the security requirement is provided as a primary means for referencing the class. The convention adopted is*: < requirement class reference> - <the first two letter of requirement name>* or similar convention.

- *Requirement Description:* a detailed description for the security requirements identified by 3GPP to reduce/counteract the risks outlined by the threat analysis.

- *Security Objective references:* a list of the short identifiers assigned to the Security Objectives achieved through fulfilling this requirement.

- *Test case:* a description of the test case that defines how the requirement is tested, the expected skills and tools to be used to produce the test outputs.

NOTE 1: The level of abstraction that should be chosen for test cases should allow implementation specific solution as long as they comply with the SCAS intention. This level of details is likely to be variable depending on the test. This work is to be done during the normative phase.

NOTE 2: Tests can consist of different types of activities. It could for example consist in reviewing documentation provided by the vendor for a given security requirement but also be of a more technical nature that will imply interaction and stimulation of the network product with a protocol testing tool for example. The concrete test activities will be defined in the normative phase.

Example of an "hardening type" security requirement:

Hardening requirements can also help to make the software/hardware of a network product more robust against un-authorized remote or physical access and can be tested as shown in the following example:

- *Requirement name***:** Unauthenticated services binding:
  - *Requirement reference:* HARDENING_BINDING.1.1.
  - *Requirement Description:* No unauthenticated services shall be bound to physically accessible ports of the network product. Unauthenticated service running on the network product and bound to physically accessible ports, even if not security related, can be used by an attacker to gain connectivity on the network product. The attacker could then try to escalate their privileges to further compromise the network product. No unauthenticated service shall be bound to physically accessible ports.
  - *Security Objective references or more general level requirement:* SO-1, SO-2, SO-3.
  - *Test case:*
    - Review the documentation provided by the vendor describing the physically accessible ports and the services bound to them.
    - Document in the report the services listening on each physically accessible port and the type of credential required for access.
    - Connect to all documented services and check that authentication is required.
    - Connect on each physically accessible port and run an appropriate scan to detect listening services on all relevant OSI layers and check whether non documented services are listening and accessible.

      or where remote scanning results are not meaningful like e.g. in case of UDP, use appropriate in-host tools to verify that only documented services are listening and accessible on the physically accessible port.

Applicability of a hardening requirement may depend on the OS or application running on the network product. E.g. in case the hardening requires removal of all non-public-key based authentication:

- Vendor A has implemented this by running the COTS component OpenSSH. Hardening for this authentication function includes e.g. disabling password based login.
- Vendor B implements this by a proprietary protocol with public and private keys, i.e. a non-COTS component. Hardening for this authentication function includes e.g. ensuring that password based authentication is not implemented or disabled.

What ultimately matters for the SECAM evaluation (compliance and vulnerability) is that the network products fulfil the security requirement (functional and hardening) and pass the related test cases, not what method was applied by the vendor to do so.

NOTE 3: To fulfil the test cases, implementation and documentation of functional requirements may also include implementation and documentation of some of the hardening requirements.

5.2.3.4 Guidelines for writing test cases

5.2.3.4.1 General

Requirements are to be testable. That is, they are to be specific enough so that a test can be written that effectively decides whether the requirement is fulfilled or not.

Some general guidelines for writing test cases are:

The test case should describe what the aim of the test is and what it is trying to demonstrate. It is not necessary to describe in details what needs to be done and what equipment is to be used. It should be left up to the lab to determine what are suitable tools and methods but it should also be specified what is suitable on high-level in order to ensure that the lab is using the right type of tools.

The test case is to match the requirement and is not allowed to extend the requirement. It is allowed that a test case may test only a subset of what is covered by the requirement as exhaustive testing may be impossible in certain cases.

Duplications should be avoided, e.g. it should be allowed to refer from one test case to (a part of) another test case already covering (part of) the requirement or to state in one test case that another test case should be run successfully before.

It should be possible to execute a test case efficiently and automation is to be preferred over manual work.

Test cases should be applicable to all elements in one or more network product classes and not assume implementation-specific details, e.g. on operating systems, that are not present in the requirement. But examples for specific environments, e.g. specific operating systems, are allowed.

The network product as defined in the present TR shall be the object on which test cases are executed. This means, in particular, that no assumptions on installing additional software, e.g. a network sniffer, on the network product are to be made.

In general, configuration changes (e.g. creating additional accounts) are to be avoided unless they are needed for the purpose of the test. But when modification of the network product is a necessary precondition for testing the requirement (e.g. when the requirement asks for configurability of the product such as in a password policy) configuration changes are allowed.

5.2.3.4.2 Verifiability and repeatability

Tests are verifiable. That is, after the test is executed there cannot be any doubt whether the test passed or failed. If there is doubt, it is a matter of opinion whether the test passed or failed which may result in unnecessary disputes. One of the purposes of the tests in SECAM is to remove opinion based verdicts of test outcome.

The detail level of a test case corresponds to the detail level of its associated requirement (see clause 5.2.3.1.1). In order to be repeatable, every test case performed with a network product needs to be described on detail level 3, i.e. specific for every individual network product. This means that the test laboratory needs to define and document test cases on detail level 3 for the security requirements on detail level 1 and 2 in the SCAS. This documentation needs to be included in the evaluation report.

Tests are repeatable when based on this documentation of test cases on detail level 3. That is, given this documentation, the network product and the corresponding SCAS, a third party should be able to repeat the tests and verify whether the network product passes or fails the test.

For a test to be verifiable, it needs to clearly specify the starting state of the system, pre-requisites for the tester, what actions are taken by the tester, and what the expected results are. The actions taken by the tester are sufficiently detailed to enable someone else to repeat the test. The expected outcome are sufficiently detailed to unambiguously determine whether the test passed or failed.

There is no need to deeply formalize how the tests are written in SECAM, but the three identified pieces of information need to be present, and they need to be clear and unambiguous:

- The initial state of the network product and pre-requisites for the tester.
- The steps taken to perform the test.

- The expected results of a successful test.

Specifying the tests clearly also helps in formulating clear requirements.

5.2.3.4.3 System under test

The SCAS applies to a network product class. In particular, the security requirements in the SCAS apply to the network product class. It is therefore important that the tests that verify whether a security requirement is met by a network product or not are mapped to the specific network product. More precisely, the expected results of the test show that the network product is acting as expected. The expected results cannot describe behavior of other network entities or personnel in the environment of the network product.

5.2.3.4.4 Template to be used for writing the test cases

Table 5.2.3.4.4-1 describes the template to be used while writing the test cases identified for each security requirement.

Table 5.2.3.4.4-1 Test case template

Test Name: *To each test case is assigned a unique name, indicating the covered topic.*
Purpose: *In this section the goal of the test (i.e. what it is intended for) should be reported*
Procedure and execution steps: *In this section the pre-conditions and the operational steps to perform the test should be reported.*
Expected Results: *In this section the expected result should be reported (i.e. the behaviour expected for the referenced requirement).*
Expected format of evidence: *In this section the expected format of the evidence should be reported. If not applicable for a specific test, then **NA** should be used.*

5.3 Improvement of SCAS and new security requirements

Vendors, operators or other bodies can propose new security requirements for addition to 3GPP SCASs if a new threat or vulnerability has been identified. This gives 3GPP the flexibility to continuously review and improve their SCASs .

6 Vendor development and product lifecycle processes and test laboratory accreditation

6.1 Overview

NOTE: The final choices and rules for the accreditation and monitoring rules are under the responsibility of the SECAM Accreditation Body. The SECAM Accreditation Body is provided by GSMA. This clause outlines what is in scope of the SECAM Accreditation Body.

The SECAM Accreditation Body describes the rules and processes for accreditation and monitoring of:

- vendor development and product lifecycle processes and
- test laboratories, whether they are vendor-owned or third-party test laboratories.

In order to be allowed conduct the evaluation in the scope of the SECAM scheme, the vendors or third-party test laboratories demonstrate they have the skills, working practices and resources to participate in the process. This is achieved by an "audit and accreditation" to evaluate and demonstrate that the test laboratories have the necessary competence, expertise, equipment, methodologies, and processes. to conduct an evaluation for conformance to 3GPP SCAS requirements.

All vendors (with or without a test laboratory) will be subject to:

- a quality qualification;
- an audit and accreditation of network product development and network product lifecycle management process.

The quality and reliability of these demonstrations are of paramount importance to the integrity of the scheme.

In order to manage the accreditations the SECAM Accreditation Body maintains a list of accredited test laboratories and vendors.

A formalized dispute resolution process for accreditation and all the other processes that are defined by the SECAM Accreditation Body is establised, as the denial or delay of accreditation may have far-reaching consequences.

A high-level overview of the processes and activities that are defined by the SECAM Accreditation Body is provided in [7].

6.2 Audit and accreditation of Vendor network product development and network product lifecycle management processes

The evaluation of the security relevant part of the Vendor network product development and network product lifecycle management processes is done as part of the vendor accreditation process by the SECAM Accreditation Body.

Vendor network product development and network product lifecycle management processes assurance requirements as well as related evaluation activities generic to all network product classes are defined by the SECAM Accreditation Body. The vendor will define their own processes and describe them in written format. During an audit, the processes will be evaluated and their application on development activities in practice will be verified. An accreditation will be awarded, if the requirements are met.

Lifecycle management consists of establishing discipline and control in the updates of network product during its development and maintenance. Lifecycle management controls are important during normal improvement of network product as well as for vulnerability/security flaw remediation (documentation used to track vulnerability/security flaw, remediation procedure with relation to corrective actions for each identified the vulnerability/security flaw…).
The vendor accreditation for network product development and network product life cycle management processes will provide assurance for these aspects in SECAM.

The Vendor network product development and network product lifecycle management processes assessment covers a vendor's engineering processes and does not necessarily apply only to a single network product. This means that the results of one assessment may apply to more than one network product. Vendors can submit their generic network product development and network product lifecycle management processes or a subset of them for auditing and accreditation. Generic network product development and network product lifecycle management processes are usually used during development of all or some products of the same vendor. As different network product development and network product lifecycle management processes could be utilized within the organization of one vendor, e.g. due to mergers or acquisitions, vendors could obtain and hold accreditation for different generic network product development and network product lifecycle management processes.

Once the vendor obtains accreditation and as long as the accreditation has not expired, vendors are allowed to produce development process compliance declarations for the "network product development and network product lifecycle management processes compliance validation" task on their own.

At the beginning of a SECAM evaluation of a product, the Vendor will have to provide a development process compliance declaration to the compliance tester containing a rationale showing that the generic accredited process was effectively applied in the network product development and network product lifecycle management of the network product under evaluation.

Requirements and accreditation procedures for vendor development lifecycle process and product lifecycle maintenance process accreditation are specified in [9].

NOTE 1: The requirements on the process and acceptable evidences as well as the procedure to obtain an accreditation for these requirements is under the responsibility of the SECAM Accreditation Body which takes into account the cost/complexity/assurance trade-off.
It is avoided that vendors need to obtain a large number of accreditations for their network product development and network product lifecycle management process. The number of requirements is relatively small (an order of magnitude of ten) to keep evaluation cost reasonable and focus on critical controls. As much as possible from existing standards is reused.

NOTE 2: The Vendor is expected to employ Industry related good working practices, e.g. aligned to the relevant parts of the ISO/IEC 27000 series. Although these areas will not be formally audited by the SECAM Accreditation Body, it is unlikely a vendor would be able to provide satisfactory evidence for meeting the SECAM requirements without having such policies and working practices in place.

6.3 Audit and accreditation of test laboratories

The accreditation is performed by the SECAM Accreditation Body, and consists of:

- assessing the skills of the vendor‘s or third-party test laboratories in conducting an evaluation for conformance to 3GPP SCAS requirements for a given network product class or range of classes;

- assessing the compliance to Test methodology (for security compliance Testing and Basic Vulnerability Testing laboratories).

A test laboratory can be accredited for any combination of 3GPP SCAS documents. During the audit for the accreditation the test laboratory demonstrates its competence, expertise, methodology and processes, to an auditor , by undertaking the tests on a concrete network product. If the test laboratory is capable of performing all the tests of the selected SCAS documents, accreditation is granted for the selected SCAS documents. Accreditation is limited to the selected SCAS documents and thereby to the respective network product classes covered by the selected SCAS documents.

Test laboratory accreditation requirements and the accreditation procedure are specified in [8].

6.4 Monitoring

The SECAM Accreditation Body monitors different kinds of accredited actors within the scheme:

- Vendors development and product lifecycle processes, which are expected to comply with the Security Assurance requirements.

- Test laboratories (for security compliance testing and Basic Vulnerability Testing), which are expected to comply with the Test Methodology and skills requirements.

Monitoring activities lead the SECAM Accreditation Body to maintain the status of these actors (accredited or not accredited).

6.5 Dispute resolution

The SECAM Accreditation Body provides a process to resolve conflicts when an accredited operator shows evidence of inconsistencies in:

- Vendor Development process activities (inconsistencies in analysis of compliance against Security assurance process).

- Test laboratories (for security compliance testing and Basic Vulnerability Testing) activities (inconsistencies in analysis of compliance against SCAS).

In the event that evaluation findings in the evaluation report are in dispute for a network product (for example: by re-doing the tests an operator finds opposite results to the ones provided by the vendors or third-party laboratories in the evaluation report), this methodology also provides a dispute resolution mechanism. This case is believed to be rare and would arise if one or several of the actors (vendors or third-party laboratories) are cheating in the evaluation or compilation of evaluation results of a 3GPP network product.

The entity responsible for deciding that a declaration should be revoked, based on the evidences and the details of the dispute procedure, is the SECAM Accreditation Body.

The dispute resolution process is specified in [10].

7 Evaluation and SCAS instantiation

7.1 Security Assurance Specification instantiation documents creation

The SCAS instantiation consist of a set of documents provided by the Vendor to give test laboratories and operators the relevant information to understand the critical parts of the network product to be evaluated. The SCAS instantiation provides a concrete mapping of the "theoretical" assets and security requirements of the SCAS into "real" assets and components supporting the security requirements of the network product being evaluated.

The SCAS instantiation is a set of documents and is not expected to have a fixed structure. This will allow vendors to maximize the reuse of existing documentation.

The content of the SCAS instantiation is however defined and it contains details on:

- Network Product description (e.g. software version, documentation version).
- Scope of evaluation.
- Mapping of SCAS security requirements to the network product and assets in the network product.
- References to the applicable document versions containing operational guidance in the documentation of the network product.
- Information needed to start the Security Compliance Testing, including Basic Vulnerability Testing.
- Details of licenses that are required for the product to operate in the scope of evaluation (if relevant).

The above document set is updated by the vendors until the testers (Security Compliance Testing, Basic Vulnerability Testing) consider they have enough and correct information to execute the required tests. Details on the content of these documents and of the update process are provided in clause 7.2.2.

7.2 Evaluation and evaluation report

7.2.1 Network product development process and network product lifecycle management

The security relevant part of the Vendor network product development and network product lifecycle management process is evaluated during an accreditation administrated by the SECAM Accreditation Body prior to any network product evaluation. During a network product evaluation, the accredited test laboratory validates that the accredited process was used for the network product under consideration. To support this evaluation, the vendor provides the following documents to the accredited test laboraty and, if requested, to the operator:

- The evidence of the vendor network product development and network product lifecycle management process accreditation by the SECAM Accreditation Body.
- The Vendor Network Product Development and network product lifecycle management process self-evaluation report for the network product under evaluation containing:

- a rationale showing that the generic accredited security relevant part of the process was effectively applied during the development of the network product under evaluation (free-form).

NOTE: Guidelines as to what constitutes valid evidence will be produced by the SECAM Accreditation Body.

The accredited test laboratory will review this self-evaluation report and evaluate if the rationale provided by the Vendor provides enough evidence that the network product is following the accredited process.

If the report is acceptable, the network product evaluation continues. If not, the test laboratory may request the vendor to provide further evidence which demonstrates compliance to the accredited vendor development and product lifecycle processes. In most cases, network product testing will be undertaken by the vendors themselves and conflict are expected to be rare. However, the test laboratories have a responsibility in this assessment as the rationale and the description of the generic accredited process will also be given to the operators who are likely to review them as well. Conflict between vendors, test laboratories and operators will be resolved by the dispute resolution process, established by the SECAM Accreditation Body [9], if one of the involved parties raises the dispute towards the SECAM Accreditation Body.

NOTE: Required and acceptable evidence for the vendor Network Product Development and network product lifecycle management process self-evaluation report are defined by the SECAM Accreditation Body to ensure comparability and facilitate dispute resolution..

7.2.2 SCAS instantiation evaluation

7.2.2.1 Overview

SCAS instantiation evaluation is to check whether a SCAS instantiation written by a vendor is a correct instantiation of the SCAS of the network product class and whether it is a good basis for evaluating the network product.

The accredited evaluator (vendor or third-party evaluator) for security compliance testing is responsible for SCAS instantiation evaluation before it is used to evaluate network product. The evaluator confirms at least that the SCAS being instantiated for a given 3GPP network product and the network product for evaluation are consistent.

7.2.2.2 Content

7.2.2.2.1 Scope of the evaluation

7.2.2.2.1.1 Overview

A given network product from a vendor might be packaged in different ways for each commercial transaction to address the tailored request from operators.

SECAM evaluations are conducted for a particular packaging of the network product. One objective in SECAM is to ensure maximum reusability of evaluation results of the evaluation of a particular package while still provide a clear and comprehensive description of the boundaries of what was evaluated. In practice to maximize the reuse, the vendor is likely to have the most commonly sold package of its network product evaluated.

A clear definition of the boundaries of what was evaluated ensures this reusability but also prevent a false perception of what was security tested as additional components are facing well-defined interfaces.

Consequently, in the scope of evaluation of the SCAS instantiation document, the vendor provides a clear description of the network product that will be tested, i.e. a description of the version of the network product in the scope of SCAS.

In particular, the network product description does not contain security requirements or functions, but a logical and physical perimeter for the evaluation. In particular the definition of the network product describes its content in terms of high level description of the components and external interfaces. This description of the network product provides:

- All components mandated by network product class definition in SCAS and implemented by the network product.

- - All external communication interfaces of the network product. Details (including protocols, ports, services and purpose) for each of the external communication interfaces of the network product that allow

communications between functions inside and outside the network product.

Finally, whether a component is part or not of the network product as well as the granularity of the definition of a component is disambiguated by the test cases of the SCAS. For example an SCAS may include the following requirement:

"Requirement: The product shall include a security audit function, accessible only by a user having the role admin X, logged through SSH on the server.

Test case:

- *the tester shall connect as the admin user through SSH and verify that he can access the audit*
- *the tester shall verify that a user without admin rights cannot access the audit using the same connection*
- *the tester shall verify that no other means exist to access the audit except a SSH session".*

In this case it is clear what, from where to test and how to test (physical port of the network product where the SSH server is listening).

NOTE 1: SECAM provides no provision to assess whether the evaluation results for a different package of the network product than the one that was evaluated are still valid. However as the boundaries of what was evaluated are made clear by the scope of evaluation clause in the SCAS instantiation, the operator can make their security acceptance decision with a clear understanding of what was evaluated for this new package.

NOTE 2: The Basic Vulnerability Testing will be conducted on the external communication interfaces of the network product.

7.2.2.2.1.2 Adapting the SCAS instantiation to special circumstances

A network product may need to adapt the SCAS instantiation to its own circumstances.

E.g. this could happen when the network product only partially implements a network product class, for which a SCAS exists. In such cases where there is no fully fitting SCAS for a SECAM evaluation the derivation in the instantiated SCAS might need some special adaptation. The possibility for adaptation is also useful to avoid that SCAS creation and Network Product Class scoping get too complex and have to cover a multitude of parallel versions with very small differences.

A SCAS instantiation might also need to be adapted when a gap is discovered in an existing SCAS, e.g. due to a newly published vulnerability, and the network product evaluation cannot wait until 3GPP has closed this gap.

7.2.2.2.1.3 Exclusion of components

The SCAS instantiation does not exclude a component from testing on the grounds that it was already evaluated under another scheme, different from SECAM, unless this SCAS allows it explicitly to refer to the certificate obtained under this different scheme for a given set of tests.

No component can be excluded from evaluation on the grounds that it was not developed by vendor itself and that it is an outsourced or a 3rd party component.

7.2.2.2.2 Mapping of SCAS security requirements to the network product and assets in the network product

The SCAS instantiation will provide:

- A concrete mapping of the SCAS "theoretical" assets to "real" assets on the network product.
- A concrete mapping of the SCAS security requirements to the high-level components supporting these functions.

The evaluator confirms at least that:

- all assets from SCAS are present in the SCAS instantiation,

EXAMPLE 1: The SCAS instantiation does not decide, against the SCAS, that some assets need no protection because of physical deployment site protection.

- if SCAS instantiation introduces new assets they are considered assets to be protected in a manner consistent with SCAS,

EXAMPLE 2: If the SCAS instantiation uses two admin roles instead of a single one in the generic SCAS, both have their credentials protected consistently.

- the SCAS instantiation does not waive threats identified in the SCAS.

EXAMPLE 3: The SCAS instantiation does not claim that a threat from the SCAS is not applicable under the assumption that more organizational control is performed during administrators' recruitment.

7.2.2.2.3 Operational guidance documents and configuration of the network product for evaluation

Operational guidance documents are part of the documentation created by the vendor and are part of the SCAS instantiation documentation (see clause 7.2.2 for details on SCAS instantiation evaluation). This documentation contains the information on how to initialize, configure and operate the network product so that SECAM security requirements are met. To achieve security, it is necessary to align the network product and the content of the "operational guidance documents".

E.g. this documentation could be a user manual indicating to the administrator:

- By default, the network product is provisioned with root password "XXXX"
- The network product will NOT be able to operate as long as this password in not changed using procedure Y
- The minimum password length is 12 characters for secure operation, at least 12 characters password SHALL be chosen

These documents will be used by:

- vendor or operator staff during initial setup of the network product.
- vendor or operator staff during operation of the network product.
- vendor or operator staff during maintenance or upgrade of the network product.
- evaluators during SECAM compliance and vulnerability evaluations to install a representative test bed.

SECAM tested configuration should reflect the setting that an administrator would choose based on these documents. To install a representative test bed, the evaluators will follow this documentation. During evaluation of a network product, no security-related initialization, configuration or operation activities other than those contained in the "operational guidance documents" will be followed; those in the documents will be followed in full.

NOTE 1: As part of SCAS instantiation documents the evaluators will evaluate these "Operational Guidance documents" and verify that these documents do not make unrealistic assumptions on the environment that waive a security requirement or a threat from SECAM and would make the test bed not representative.

NOTE 2: In the scope of SCEAM it is implicitly mandatory for the vendor to consider the security requirements defined in SECAM for creating the operational guidance documents. If relevant initialization, configuration and operation instructions were missing from the operational guidance documents then the network product will inevitably fail the test cases for the respective security requirements.

7.2.2.2.4 Information needed to execute the required tests for SCT and BVT activities

Information needed to execute the required tests for the Security Compliance Testing:

The compliance tester assesses whether the SCAS instantiation contains enough information to:

- execute the test cases;

- determine whether the tests completely and accurately cover the SCAS.

In cases where the SCAS instantiation does not include enough information, the compliance tester can ask the vendor to modify/complete the SCAS instantiation.

Information needed to execute the required tests for the Basic Vulnerability Testing:

The basic vulnerability tester assesses whether the SCAS instantiation contains enough information to:

- determine the tools to be used in the Basic Vulnerability Testing;
- execute the test cases;
- determine whether all open ports are explicitly documented;
- determine the scope of vulnerability scanning to reflect the SCAS requirements.

In cases where the SCAS instantiation does not include enough information, the BVT tester could ask the vendor to modify/complete the SCAS instantiation.

7.2.2.3 Process

The usage and update of this set of document during a SECAM evaluation is described in figure 7.2.2.3-1 below.

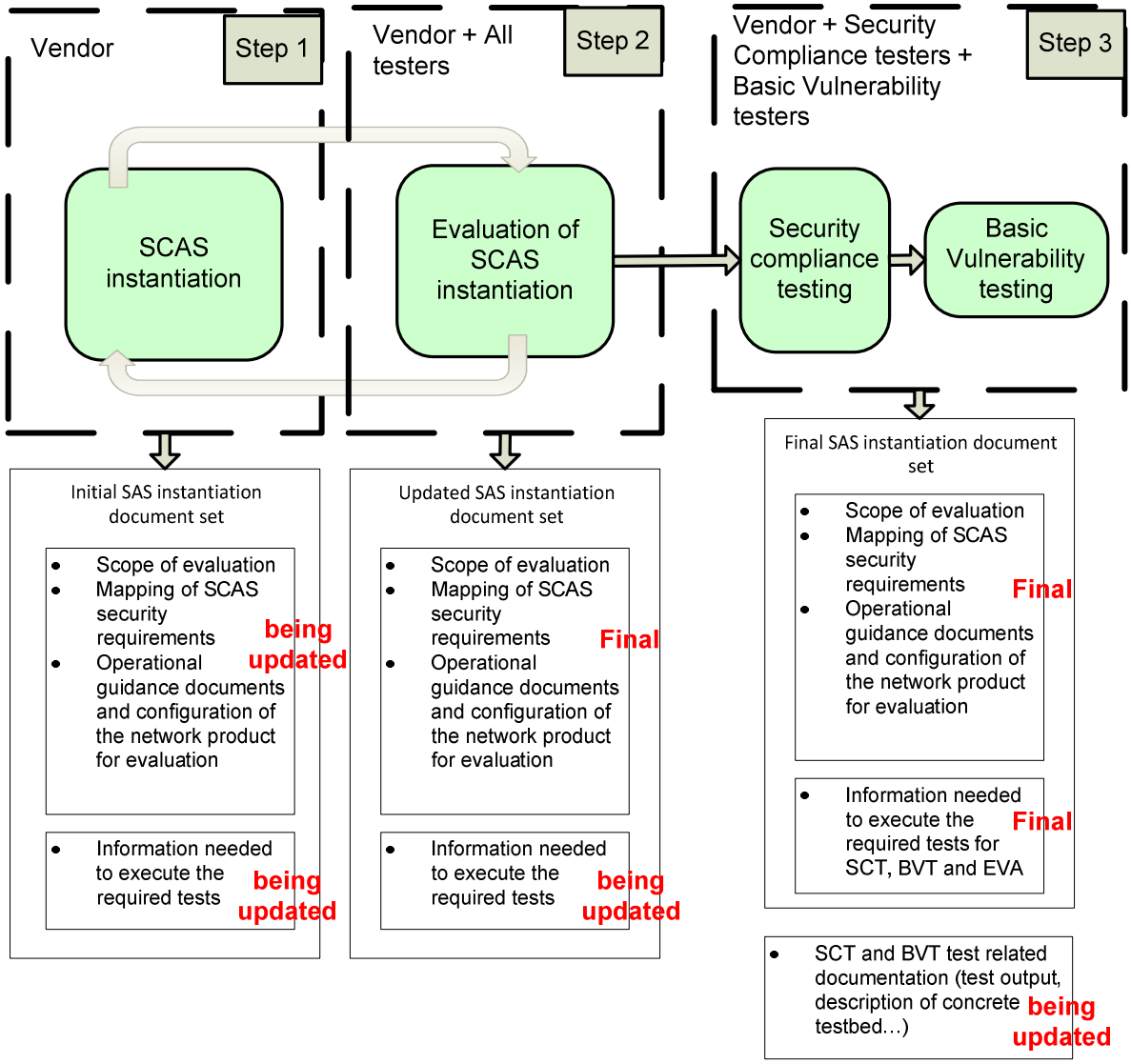

Figure 7.2.2.3-1: Overview of the SCAS instantiation documents evolution during a SECAM evaluation

Step1 is the initial production by the vendor of the required documentation and its update if required by step 2. It is outside of the scope of SECAM to describe this task.

Step 2 is the SCAS instantiation evaluation to check whether an SCAS instantiation written by a vendor is a correct instantiation of the SCAS of the network product class and whether it is a good basis for evaluating the network product.

Step 3 is about performing the SCT and BVT testing tasks as described in the present document. which will use this instantiation documentation as input. The evaluation does not start (neither SCT nor BVT) as long as steps 1 and 2 are not completed.

Further documentation is produced during step 3 . During step 3 for example, the SCT and BVT testers will describe the concrete test bed used for testing as well as "instantiated test cases" (i.e. the description of the concrete test case on the network product corresponding to the generic SCAS test case). At the end of step 3, the SCAS instantiation documentation as well as the SCT and BVT documentation is an output document provided to the operator. These documents are described in clauses 7.2.3 and 7.2.4.

After step 3, the SCAS instantiation documentation as well as the SCT and BVT documentation produced in step 3 are given to the operator for its final review and final security acceptance decision.

7.2.3 Security compliance testing

7.2.3.1 Inputs

The test bed configured according to the documentation that was produced in step 3 of clause 7.2.2.3.

7.2.3.2 Outputs

In the end of Security Compliance tests, the tester delivers a Security Compliance Testing report which includes:

- a declaration about who carried out the tests;
- network products/features tested and reasons for not testing where applicable:
  - in particular, copies of other Security Compliance related third party certificates and test reports of previous evaluation (internal and/or third party), if appropriate and available;

NOTE: Whether SECAM recognizes the results of other evaluation schemes, so the Security Compliance tester can avoid re-testing previously evaluated items, will be decided in the normative phase requirement per requirement. For example, if there is a requirement to implement AES-256 encryption for a component, SECAM might accept a FIPS evaluation of the cryptographic module as a valid test result and might not ask the Security Compliance tester to verify again (source code review, test vectors…) that AES-256 is indeed implemented.

- a description of the testbed used for the tests, which are
  - accurate,
  - make the test bed reproducible (non ambiguous),
  - representative of real-life network product deployment;
- the test tools and vectors used for the tests;
- a rationale which demonstrates that the tests cover the SCAS test cases;
- the test procedure followed in practice (following SCAS test cases) and results (following SCAS output format indications).

7.2.3.3 Activities

The security compliance of a network product is its compliance to a defined set of security requirements. The security requirements set will be provided in the SCAS. The test case describes the validation technique to be used by the Security Compliance Test laboratories as well as the expected outputs to provide in the evaluation report.

Security compliance test laboratories execute the tests contained in the 3GPP SCAS for the evaluated network product as described in the test cases, collect evaluation evidences and include them in the final security compliance testing report (see clause 7.2.3.2 above for details of outputs).

NOTE: The test results and data may be collected from test execution instance run by the vendor test team as part of its product development cycle.

7.2.4 Basic Vulnerability Testing

Basic Vulnerability Testing activities consist of requirements for running automated Free and Open Source Software (FOSS) and Commercial off-the-shelf (COTS) security testing tools against the external interfaces of a Network Product. Such tools or equivalent alternatives are likely available to all kind of attackers.

NOTE 1: As Basic Vulnerability Testing is universally applicable for all Network Product Classes, the requirements for this testing category are specified as a general SCAS module. This general SCAS module will then be linked and potentially amended by SCASs for individual Network Product Classes.

NOTE 2: The requirements in this testing category are kept general, the wildcard (protocol) indicates a placeholder for the actual protocol relevant as it is implemented in the Network Product and made available on external interfaces. Unless specified otherwise during the normative phase BVT applies to all interfaces providing IP-based protocols.

NOTE 3: The individual tools used for Basic Vulnerability Testing are selected by the Security Compliance Test laboratories. The SECAM Accreditation Body will ensure during laboratory accreditation that the testers are able to utilize adequate tools.

NOTE 4: To avoid creating a monopoly for security testing tool vendors the usage of a security testing tool having specific capabilities should only be mandatory if there are at least two alternatives by different vendors available for use in most world regions.

This activity covers at least three aspects: Port Scanning, Vulnerability Scanner by the use of Vulnerability scanners and robustness/fuzz testing. The tester delivers a Basic Vulnerability Testing report which includes:

- the test procedures (following SCAS);
- the test results (following SCAS output format indications).

7.3 Self-declaration

After the evaluation process is finished, the vendors review all the evaluation results of the product and give a declaration of their product. In the self-declaration, vendors should:

- give a short summary and conclusion of all the evaluation reports;
- declare all tests conducted by the vendors are correctly carried out and all the documents provided by the vendors are authentic without intentional deception.

7.4 Partial compliance and use of SECAM requirements in network product development cycle

The vendor is likely to integrate SECAM requirements and test cases in its continuous development process. During this phase, a given network product might fail fully or partially some of the SECAM compliance and/or vulnerability test. The process of how and when vendor choose to fix or not to fix this network product before the final evaluation is under vendor's responsibility and is outside of SECAM scope.

SECAM scheme describes the final evaluation for the final network product version expected to be bought by operators. SECAM encourages vendors to aim at a full compliance of all SECAM requirements which should represent a minimum baseline. However, the final network product might still only partially fulfil SECAM requirements. This partial compliance will be documented in the test results in the evaluation report. The final security acceptance decision is under operators' control which might accept partially compliant products. This choice is under operators' responsibility and is outside of SECAM scope.

7.5 Comparison between two SECAM evaluations

SECAM evaluation considers a given version of a network product. SECAM documents don't describe or evaluate the improvement between two evaluations of the same version of the network product.

7.6 The evaluation of a new version

After a network product completes a SECAM evaluation by a test laboratory, the vendor may upgrade the network product e.g. as a result of modified features, remediation of vulnerabilities etc. A re-evaluation of the new version of the network product can be carried out in two ways as described below:

- evaluation as per a new product by using all the test cases as defined in the SCAS’s;

- the vendor provides a detailed list of the updates to the product and provides a list of related test cases that will verify the new version of the product. Once the vendor and the test laboratory agree on the updated test plan, the evaluation takes place.

  On completion of the evaluation the test laboratory will include in the evaluation report:

  the list of updates to the network product.

  Test cases that were executed in the evaluation.

  The test results from the evaluation.

  Operators can then decide on accepting a compliance statement for the updated version of a network product.

Editor's Note: It is ffs whether there should be a limit on the number of allowed delta changes before a complete re-evaluation of the product is required and, if so, what this limit should be.

Annex A:
Summary of SECAM documents

Phase	Sub-phase	Deliverable	Published by
Methodology building		Consensus on threats	3GPP
		Security Assurance process	
		Security Assurance Specifications	
		Test methodology and skills requirements	SECAM Accreditation Body / GSMA
		Test laboratories accreditation and monitoring rules	
		Network product development and network product lifecycle management Process Assurance requirements	
Accreditation	Methodology Accreditation	Accreditation report	Accreditor
	Audit and accreditation	Evidence of successful accreditation of vendor network product development and network product lifecycle management process Evidence of successful accreditation of Security Compliance test laboratories Evidence of successful accreditation of Basic Vulnerability Test laboratories	SECAM Accreditation Body / GSMA
Evaluation	SCAS instantiation	Instantiation of SCAS	Vendor
	Vendors Development process compliance	For the accreditation: Design documentation [free-form] Operational guidance [free-form] Version and configuration management plan [free-form] Flaw remediation documentation [free-form] Process to ensure code quality documentation [free-form] Vendor's development sites protection [free form] Before any network product evaluation: Network Product Development and network product lifecycle management process self-evaluation report providing evidences that the network product was developed under the accredited process [free-form]	
	Security compliance testing	Security Compliance Testing report	Vendor or third-party
	Basic Vulnerability Testing	Basic Vulnerability Testing report	
Self-declaration	Self-declaration	Self-declaration	Vendor
Monitoring, dispute resolution		Informal guidance document. Accreditation revocation list	SECAM Accreditation Body / GSMA
Dispute resolution	-	Operator claims	

Annex B:
Summary of actors involved in SECAM

Actor	Tasks and Responsibilities
3GPP	Describe SECAM in the security assurance process documentation (i.e. the present document) Provide SCASes for individual Network Product Classes: - **Describe and model the network product class:** Compile a complete list of features/capabilities considered relevant for evaluation - **Define the security problem:** Identify which assets in the model of the network product class require protection and how these assets can be exploited by an attacker. The security problem definition also contains the security objectives of the network product class under analysis (i.e. which assets require what type of protection), and defines an attacker potential the network product class is supposed to resist. Also, undertaking of a threat analysis - **Identify the security requirements and test cases:** Detail security requirements to reduce/counteract the risks outlined by the threat analysis as well as a description of the test cases and where possible with expected test results. Or, detail environment assumptions to countermeasure to mitigate the risks. - **Verify the Security Requirements:** Once the security requirements have been identified it is verified that the security objectives are met by these security requirements, and that every security requirement contributes to defending an identified security objective. Define the expected skills and tools for security compliance test laboratories based on the Security Functional Requirements in the SCASes. Specify general Basic Vulnerability Testing requirements as a SCAS module. This general SCAS module will then be linked and potentially amended by SCASs for individual Network Product Classes. This SCAS module does not specify individual tools but rather BVT categories and the conditions under which the usage of suitable tools are required.
SECAM Accreditation Body	Describe the rules for accreditation and monitoring of development and test laboratories. Develop Vendor network product development and network product lifecycle management process assurance requirements as well as related evaluation activities generic to all network product classes in a dedicated document. Assess the skills of the test laboratory in conducting an evaluation for conformance to 3GPP SCAS requirements for a given network product class or range of classes; This includes assessing the test laboratory's skill in selecting tools for performing the evaluation. Assess the test laboratory's ability to comply with the test methodology (for security compliance Testing and Basic Vulnerability Testing laboratories). Administer the evaluation of the security relevant part of the Vendor network product development and network product lifecycle management process during an initial accreditation. Provide a process to resolve conflicts.
(Accredited) Vendor	Ensure Vendor network product development and network product lifecycle management process assurance compliance. Provide SCAS instantiation document. Provide self-declaration after evaluation: - give a short summary and conclusion of all the evaluation reports - declare all tests conducted by the vendors are correctly carried out and all the documents provided by the vendors are authentic without intentional deception.
(Accredited) Vendor or (accredited) third-party Test laboratory	**All Test laboratories:** - Assess that the vendor documentation and processes are complete sufficiently defined to begin the evaluation - Validate the elements (scope of evaluation, instantiated assets…) which will not be modified during the evaluation Special for **Security compliance testing Test laboratories:** - Check whether a SCAS instantiation written by a vendor is a correct instantiation of the SCAS of the network product class and whether it is a good basis for evaluating the network product. - Confirm that the SCAS being instantiated for a given 3GPP network product and the network product for evaluation are consistent. - Do Security Compliance Testing according to SCAS instantiation. - Deliver Security Compliance Testing report (cf.clause 7.2.3.2) For **Basic Vulnerability Testing Test laboratories:** - Do Basic Vulnerability Testing. - Deliver Basic Vulnerability Testing report (cf.clause 7.2.4)
Operator	**Operator security acceptance decision:** Examines the network product, the compliance reports and the test laboratories accreditation published by the SECAM Accreditation Body and decides if the results are sufficient according to its internal policies.

Annex C:
Change history

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
2017-03	SA#75	SP-170104	0001	-	B	Adding evaluation of a new version of a 3GPP network product to TR 33.916	14.1.0
2017-06	SA#76	SP-170431	0002	-	F	Update of references to GSMA NESAS documents in TR 33.916	14.2.0
2017-06	SA#76	SP-170431	0003	-	F	Deletion of editor's note in 33.916	14.2.0
2018-03	SA#79	SP-180123	0004	1	F	Collection of changes based on feedback from GSMA SECAG	14.3.0

History

Document history		
V14.1.0	April 2017	Publication
V14.2.0	July 2017	Publication
V14.3.0	April 2018	Publication