3GPP TR 33.805 V1.2.1 (2013-09)

Technical Report

3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Study on Security Assurance Methodology for 3GPP network products (Release 12)

Keywords
LTE, UMTS, GSM, security, assurance, security evaluation

3GPP

Postal address

3GPP support office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet
http://www.3gpp.org

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 studies methodologies for specifying network product security assurance and hardening requirements, with associated test cases when feasible, of 3GPP network products. Network product security assurance and hardening refers to protection against unwanted access to a 3GPP network product, its Operating System, and main running Application(s). The suitability of industry standard methodologies and the potential need for collaboration with bodies such as GSMA, CCRA, ISO and ITU will be assessed. The study will also consider regulatory aspects and the potential need for security certification. The suitability of the candidate methodologies will be assessed with reference to real world examples.

Part of the scope of this work is to conclude which 3GPP network products, if not all, would be subject to 3GPP network product security assurance and hardening requirements. There is likely to be a long list with the result that prioritisation will be required. LTE network product classes will be the first priority. The work will also study exactly what should constitute a 3GPP network product in the context of this study e.g. whether it should be an individual 3GPP functional entity, a group of 3GPP functional entities or some other realisation.

The study will also include assessing the extent to which individual 3GPP network products need to be hardened beyond a common baseline and should take into consideration network vs. environment.

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] GISFI_SP_201206260: "Report on Common Criteria".

[3] The CC and CEM documents: http://www.commoncriteriaportal.org/cc/

[4] The CCRA introduction: http://www.commoncriteriaportal.org/ccra

[5] CCRA Licensed Laboratories: http://www.commoncriteriaportal.org/labs/

[6] On Certificate Authorizing and Consuming nation: http://www.commoncriteria-india.gov.in/Pages/InternationalPartners.aspx

[7] CCRA certified products and PPs: http://www.commoncriteriaportal.org/products/ ; http://www.commoncriteriaportal.org/pps/

[8] 3GPP TS 33.401: "3GPP System Architecture Evolution (SAE); Security architecture".

[9] 3GPP TS 33.402: "3GPP System Architecture Evolution (SAE); Security aspects of non-3GPP accesses".

[10] 3GPP TS 23.401: "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access".

[11] 3GPP TS 23.402: "Architecture enhancements for non-3GPP accesses".

[12] 3GPP TS 33.310: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Network Domain Security (NDS); Authentication Framework (AF)".

[13] 3GPP TS 33.320: "Security of Home Node B (HNB) / Home evolved Node B (HeNB)".

[14] CCRA Supporting documents: http://www.commoncriteriaportal.org/supporting/

[15] Common Criteria for Information Technology Security Evaluation, Version 3.1 Release 4, September 2012
http://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R4.pdf
http://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R4.pdf
http://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R4.pdf

[16] General-Purpose Operating System Protection Profile, DRAFT, Version 3.9
http://www.niap-ccevs.org/pp/pp_gpos_v3.9.pdf

[17] U.S. Government Approved Protection Profile – Protection Profile for Network Devices (NDPP), 08 June 2012. http://www.niap-ccevs.org/pp/pp_nd_v1.1.pdf

[18] CPA Build Standard v1.2–
http://www.cesg.gov.uk/Publications/Documents/the_cpa_build_standard.pdf

[19] 3GPP TS 33.210: "3G security; Network Domain Security (NDS); IP network layer security".

[20] "3GPP TR 33.821: "Rationale and track of security decisions in Long Term Evolution (LTE) RAN / 3GPP System Architecture Evolution (SAE)".

[21] "3GPP TS 33.102: "3G security; Security architecture".

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].

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

3GPP Security Assurance Methodology (SECAM): The 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 testing laboratory is impartial and competent to carry out specific tests or types of assessments. In the context of SECAM, it would be recognition that a testing laboratory is competent to assess the 3GPP network product against the requirements from the 3GPP SAS and to produce an evaluation report.

NOTE 1: If an accreditation body is not chosen for SECAM by 3GPP or GSMA (TBD), it will not be possible to know how widely the evaluation results will be recognized. For example, if the accreditation lab chosen by a vendor for evaluation (self-evaluation or third-party evaluation) is not recognized by a country where the products are to be sold, then the evaluation results would become equivalent to self-evaluation without accreditation in this country.

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.

Evaluation without accreditation: Evaluation as defined below in self-evaluation or third-party evaluation but without accreditation of the labs in the country where the Security Assurance process is required.

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.

Certification: Certification is the confirmation by an independent Certification Authority (CA) that the evaluation has been properly carried out. That is, a confirmation that the evaluation criteria, evaluation methods and other procedures have been correctly applied and that the conclusions of the evaluation report are consistent with the evidence adduced. The CA does not test the network product or verify the security functionality of the network product. The CA examines the evaluation report. If the CA finds the evaluation report satisfactory, it issues a certificate stating this fact.

Certificate: The certificate is the official document attesting that the evaluation of the 3GPP network product against the 3GPP Security Assurance Specifications (SAS) was conducted correctly and was successful. This document is provided by the third-party certification authority. The certificate provides the value that an operator that trusts the Certification Authority (CA) can feel more assured about that the network product fulfils the claimed security level.

Evaluator: evaluates the network product and produces an evaluation report. The vendor, the operator, GSMA, NVIOT, 3GPP, GCF or some other party, could take the evaluator role.

Auditee: The Auditee is the 3GPP network product vendor who is to be evaluated. The Auditee is responsible for supplying all necessary information to the evaluators at the beginning of the evaluation.

Certification Authority (CA): the entity responsible for the certification process.

Accreditation Authority: the entity responsible for the accreditation process.

Assurance: is the confidence that a network product meets its specific security objectives. Assurance is usually verified by performing an evaluation.

Assurance level: is related to 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 2: At this point the "3GPP Assurance Levels" have nothing to do with "Evaluated Assurance Levels" used in Common Criteria. It is for further study how and even if the two map.

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.

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.

NOTE 3: It is for further study if and how "3GPP Security baselines" take account of and map to those used in other schemes for example the Basic, Medium, and High "Robustness Levels" in NSA NIST.

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.

Security Compliance Testing (SCT): Evaluation process step used in Methodology 2 to describe activities for checking the compliance of a network product with applicable Security Assurance Specifications (SAS).

Basic Vulnerability Testing (BVT): The process of running security tools against a network product. In Methodology 2, 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. Details on these tools can be found in Annex A.2.1.

Enhanced Vulnerability Testing (EVA): Evaluation process step used in Methodology 2 and described in clause 5.2.4.5. This activity takes the output of the earlier Security Compliance Testing (SCT) and Basic Vulnerability Testing (BVT) into account.

NOTE 4: The exact scope and activities of EVA is FFS in a future Study Item. Examples include more advanced activities than executed during the Basic Vulnerability Testing (BVT) stage and chaining of vulnerabilities to penetrate the tested system. EVA may depend highly on the skills of the testers.

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

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].

BVT	Basic Vulnerability Testing
CA	Certification Authority
CC	Common Criteria
COTS	Commercial off-the-shelf
EAL	Evaluation Assurance Level
EVA	Enhanced Vulnerability Testing
FOSS	Free and Open Source Software
ITSEF	Information Technology Security Evaluation Facility
PP	Protection Profile
SAS	3GPP Security Assurance Specification
SAR	Security Assurance Requirements
SFR	Security Functional Requirements
SGSN	Serving GPRS Support Node
SCT	Security Compliance Testing
SECAM	Security Assurance Methodology
ST	Security Target
TCSEC	Trusted Computer System Evaluation Criteria
TOE	Target Of Evaluation
VA	Vulnerability Assessment

4 3GPP network products and threat model

4.1 Considerations on definition of the term "network products"

4.1.1 3GPP function specific requirements vs. platform/node requirements

A SAS will be produced with some specific target in mind, this target being related to the realization of some 3GPP defined functionality. For example, if the 3GPP function SGSN is implemented on a server platform, a SAS may have a security requirement that the software updates to the server platform where the SGSN function is running shall be integrity protected. However, the SGSN function as defined in 3GPP does not have a defined capability for updates to the server platform. Therefore such a requirement cannot be put on the SGSN seen as a function. The server platform here includes the hardware components, the operating system, etc.

However, in the end, 3GPP functions are implemented in one platform or another and this must be taken into account in this study.

There is hence a need to distinguish between at least two types of requirements for the purpose of the discussion in this clause. These two types are platform requirements that relate to the hardware and operating system, and 3GPP function requirements that relate to protocol behaviour defined in 3GPP technical specifications. There may be further subdivision of these requirements, e.g., the platform requirements may be subdivided into hardware related requirements and requirements related to secure boot etc. However that is not necessary for the discussion in this clause.

4.1.2 Distribution of 3GPP functions over nodes

For simplicity, a physical entity implementing one or more 3GPP functions will be referred to as a node in the clause 4.1.

One node – many functions

3GPP mainly defines logical functions. For example, an SGSN and an MME are two 3GPP functions in the 3GPP architecture. Often they are thought of as two different nodes. However, it may in some cases be advantageous to implement these two 3GPP functions in the same node. Other examples of co-location are when the RNC 3GPP function is implemented in the same node as a NodeB 3GPP function. In fact, an entire mobile network may be implemented in the same node. The latter is sometimes referred to as "network-in-a-box" and can be useful in situations where fast deployment is necessary, e.g., in catastrophe areas.

One 3GPP function – many nodes

Coming from the other direction, it is also common that the implementation of a single 3GPP function is split over several nodes. An example is the HSS. The HSS may be split so that there are a set of back end databases storing the subscription data and a set of front ends that implement the protocol interfaces toward other functions, such as the MME. The back ends and the front ends may be implemented in separate physical nodes. This is treated as an implementation detail in the 3GPP specifications and should be continued to be treated as such for flexibility.

Observations

- **More than one SAS may apply to a particular node**. A situation where this will occur is for example where the RNC 3GPP function is co-located with the NodeB. Already today the specifications require more security from RNCs in so-called vulnerable locations than from RNCs in more secure locations.
- **Depending on implementation, a SAS may not apply to the entire 3GPP function**. A situation where this may occur is the HSS example from above. The AuC most likely will have much harder requirements than other parts of the HSS. It may not be necessary to require the same strong security for all parts of the HSS since this will unnecessarily raise the cost of these nodes.
- **One SAS per 3GPP function lead to too many SASs**. There are too many 3GPP functions in the 3GPP architecture to have one SAS per function. Combinations of 3GPP functions and platform requirements make this problem even larger. One SAS must hence cover more than one 3GPP function. 3GPP functions that are similar, for some definition of "similar", must be grouped together for this to be manageable.

4.1.3 Environment of functions and nodes

Physical location of functions and nodes

3GPP functions in the core network have traditionally been considered to be placed in secure location. Their locations are considered trusted to not be physically accessible to attackers. Functions and nodes physically located in secure locations, such as in the core network, must be considered to be safe from physical tampering. The requirements on functions/nodes in the RAN may in most cases not make this assumption.

A problem is that functions may not always be located in the core network. Depending on implementation, they may be located in the RAN or in third-party facilities and locations. Therefore more than one type of SAS may apply to a single function (if that is the chosen target) depending on the deployment of the function. For example, one SAS module could describe requirements for only the physical protection of a function/node, whereas a second SAS module may describe the requirements for only the function provided. If the node is built to be located in a physically vulnerable location then the first SAS and the second SAS are applied. If the node is built to be located in physically secure location, then only the second SAS is applied

For example, RNCs located in so called exposed locations are required to implement IPsec to protect the backhaul just like eNBs, whereas when the RNC is not in an exposed location the requirement on IPsec would not always be necessary when the Iu interface could be assumed to be physically secured (cf TS 33.210 [19]).

Another example is that Network Functions Virtualisation products (such as virtual MME, virtual HSS and virtual Firewall, etc.) may be installed on a third-party Internet Data Center (IDC) facility which is a so-called “non-trusted domain”. In this case, it should be required that encryption be applied on data transmission and data storage, so that an operator’s operation and maintenance data are properly protected.

Remote exposure of functions/nodes in the network architecture

3GPP functions of which at least one interface is accessible from outside the network security domain can be considered to be in a more hostile location than nodes assumed to be only accessible from within the network security domain. For example, a PGW is accessible from some PDN, and can then be attacked via this network. To prevent this attack, a firewall might be needed. But in case there is no firewall, the PGW is required to properly filter incoming traffic. Therefore, the network architecture and remote accessibility significantly influences security requirements.

NOTE: None of the definitions of remote accessibility and physical location are complete until the attacker model is defined.

Figure 4.1.3-1 describes possible combinations of remote and physical exposure.

Editor's note: It is FFS whether security measures should be taken into account when determining the degree of exposure according to the definitions above.

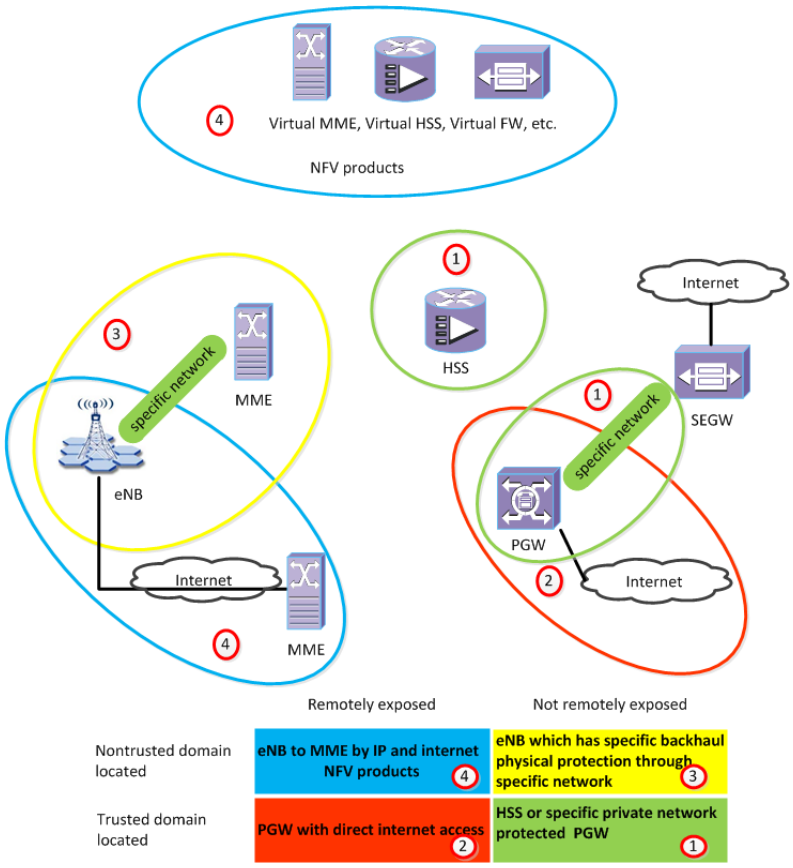


Figure 4.1.3-1: Environment of 3GPP network products

NOTE: It might be meaningful to use the original terms "physically exposed" and "physically unexposed" in certain contexts for easy understanding instead of "trusted and non-trusted domain located". For example, when necessary, we can say: "RNC is located in an exposed location (which is in an un-trusted domain)."

Consequences

From the above analysis, the environment needs to be taken into account when defining the SAS to be applied to a particular network product. The word "environment" refers to the location in a trusted domain such as HSS in a physically unexposed location, or the location in a non-trusted domain such as RNC in a physically exposed location. The word "environment" may also refer to the remote exposure case. To sum up all possible differentiation aspects could become an intractable task, if playing with the full range of threat or location parameters. Instead, robustness against some uncertainty and variability in the environment shall prevail.

4.1.4 Relationship between network products classes, SAS and 3GPP functions

1. When defining a network product class, it needs to be defined which 3GPP functional entities or part of 3GPP functional entities are within this network product class

2. SAS 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. The assumption is that this modularity will allow a reasonable number of SAS.

3. In a third step, it would be decided which SAS modules apply to which network product classes

Editor's Note: It is FFS in which cases these additional SAS modules will be optional or mandatory.

There will be a single SAS for a given network product class. The standardization will start with a given network product class for consideration (for example an RNC). During the threat analysis phase, an agreed level of exposure for the network product class under consideration will be chosen. If no agreement can be found on the exposure level, it is likely to be because the initial definition of the network product class under consideration was too wide, for example

because RNC class also included so called collapse RNC/NBs which have a too different exposure level from classical RNCs.

In this case a new network product class will be created on the fly: e.g. collapsed RNC/NBs would be a different class from classical RNCs. This is aligned with the assumption of a single SAS per network product class.

4.2 Sample 3GPP network products for the methodology study

One of the goals of this study is to choose a methodology for specifying network product security assurance and hardening requirements, with associated test cases when feasible, on 3GPP network products. In order to choose this methodology, it is not needed to validate the methodology on all 3GPP network products as it would make the study unnecessarily long.

Clause 4.1 describes the aspects to be considered in order to choose relevant sample for the methodology evaluation:

- Distribution of 3GPP functions over nodes
- 3GPP function specific requirements vs. platform/node requirements
- Location of function and nodes

To address the last bullet, one example in an exposed location and one in the core network will be considered. To address the first two bullets, one example implementing two 3GPP functions will be considered.

NOTE: For the purpose of this study, it will be considered that these network products are owned and managed by a single operator.

Core network product class:

The core network 3GPP functions to be used as an example for the study will be the SGSN and the MME ones, in a form of a physically combined SGSN/MME.

Exposed location network product class:

The exposed 3GPP function to be used as an example for the study will be an eNodeB.

4.3 Threat and attacker model for the Security Assurance study

4.3.1 Attacker potential

The security functions needed to reach a given level of resistance are dependent on the abilities of presumed attackers. The more powerful and knowledgeable potential attackers are, the more and stronger security measures are needed to counter the types of attacks these attackers might launch.

One aspect to consider is the location/environment of the 3GPP-defined functionality.
In an exposed location/environment it becomes difficult to rule out any specific form of attacker.
In a highly protected location on the other hand, the only potential attackers with physical access are insiders.
Insiders are often more knowledgeable than outsiders about technical properties (e.g. implementation details) of the 3GPP-defined functionalities. It is common to mitigate the risk of insider attacks by, amongst other methods, organizational policies or vetting of employees - in which case no additional technical means of defence are usually needed. However, in some situations (e.g. access through 3rd party maintenance personnel), it may be necessary to consider additional security measures mitigating the risk of insider attacks.

In order to be able to assure that a sufficient security level is met, 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.

4.3.2 Threats model

There are many threat and risks analysis or modelling framework available for IT equipment and computers networks.
SECAM will cover threats related to 3GPP functions as well as threats related to generic IT functions.
None of the framework is likely to perfectly fit the needs of SECAM which ultimate goal is to be capable to derive concrete and testable security requirements to reduce the level of exposure of telecom equipment.

Having a look at these threat modelling/analysis frameworks to identify the main threats categories/attack paths will help 3GPP SA3 to move faster for this step of writing the threat and risk analysis in the normative phase of SECAM.
It is however not a pre-requisite for deciding on the SECAM methodology and for moving in the normative phase.

Annex D provides description of different alternative framework that could help to structure the work.

4.4 3GPP network products subject to Security Assurance Specifications (SAS)

4.4.1 Access network

For this study the following access network product is in the scope:

- eNodeB

NOTE: SECAM Security Assurance Specification will cover network product classes. There is no reason to assume that SECAM evaluation would not be applicable to specific form factors of base stations (metrocells, microcells) as long as the functions and interfaces of these small form factor base stations are the same as the ones of an eNodeB network product class.

- H(e)NodeB

NOTE: Considering that H(e)NBs rely on a different security architecture with a different functional split, they are considered as a different network product class for SECAM.

4.4.2 Core network

For this study the following core network products are in the scope:

- Mobility Management Entity (MME)
- Serving GPRS Support Node (SGSN)
- Serving Gateway (S-GW)
- PDN Gateway (PDN GW)
- Security Gateway
- Home Subscriber Server (HSS)
- PCRF
- AAA server

NOTE: AAA Server should be in the scope of this study because they can be reachable from equipment not belonging to the internal Mobile Network.

- Operation and Maintenance Servers/Applications (OAM Servers/Applications)
- Call Session Control Function (CSCF)

Editor's note: Whether other classes of IMS network products will be included is FFS.

4.5 Roles and processes applicable to all methodologies

4.5.1 Introduction

This clause describes the most important elements, roles and processes from which the security assurance process is built. The clause also describes how these components fit together in the security assurance process.
The process is independent from the methodology chosen. It does, however, impose requirements on what the methodology has to provide, i.e., each methodology shall define how an evaluation is performed and optionally how the certification step is performed.

In clause 4.5.2, the process is described without defining which party takes on which role.
Clause 4.5.3 defines the different roles, and finally, clause 4.5.4 defines the steps in the process in more detail and the inputs and outputs to these steps.

The current business environment implicitly defines some of the roles and steps in the security assurance process. The reason for this is that there are informal and less rigorous security assurance processes for 3GPP related products already today. For example, the start and end of the process are already defined; the vendor produces the network product and the operator decides to accept or reject the provided assurance regarding security of the network product. These existing processes are vendor and operator specific.

NOTE: The description of the legal framework for the evaluation/certification process is outside of the scope of SA3.

4.5.2 Security assurance process

4.5.2.1 Overview

The security assurance process describes how the operator gets assurance regarding the security of the network product. The process is depicted in Figure 4.5.2.1-1. 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 (SASs) that the network product is aiming to fulfil. Choice of which SASs to select may depend on operator and/or regulatory input. Then the product is evaluated against the Security Assurance Specification(s). During this step, information may need to be exchanged between the evaluator, the vendor and/or the operator. The evaluation results in an evaluation report. The roles are described in clause 4.5.3; see that clause for a definition of the evaluator role.

There are two alternatives how to proceed from this point. The choice of alternative depends on whether the operator requires a certification to accept the evaluation or not. If the operator requires certification of the evaluation, a certification authority has to examine the evaluation report and issue a certificate if satisfied. If, on the other hand, the operator does not require certification, the certification can be ignored and the operator receives only the evaluation report. Note that the party doing the evaluation may be the same party that issues a certificate. However, since certification is only an optional addition in the process, it is beneficial to separate the evaluator role and the certification authority role; see clause 4.5.3 for further descriptions of the roles.

Editor's note: The content of the evaluation report and the confidentiality issues associated to it are FFS.

Once the operator received the evaluation report, and possibly an indication of whether the network product passed certification, the operator takes a decision to either 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.

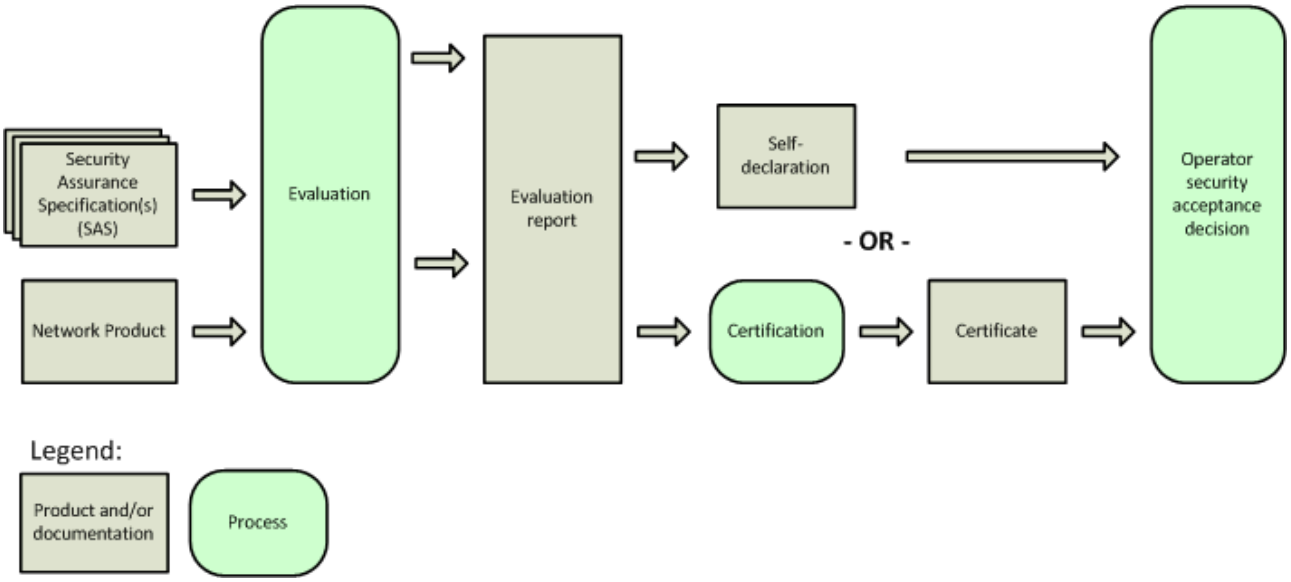


Figure 4.5.2.1-1 Security assurance process.
The text "- OR -" in the figure indicates that the evaluation report may be provided directly to the operator or that it may be subject to certification first.

The certification step is optional for use in addition to being optional to be defined by the methodology.

NOTE: A commonly used term in the context of certification is so called "self-certification". Since this technical report needs to use more granular concepts, such as self-evaluation with and without accreditation in combination with self-declaration, third-party evaluation in combination with self-declaration etc., the term "self-certification" is too coarse and hence not applicable. However, this does not rule out that self-evaluation without certification can be performed.

Naturally, this is an idealized process description. In reality, there may be iterations of the process or iterations of parts of the process. For example, when the vendor provides an update impacting major functions of the network product, the existing evaluation report may have to be updated. Following that, possibly a re-certification and a new operator acceptance decision has to be taken.

4.5.2.2 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 evaluator 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 will be constant: SECAM intends to provide 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 Target Of Evaluation (TOE) resistance. For example, if an attacker were believed to have knowledge of TOE implementation, a black box assessment only would be unreasonable

NOTE: Many notions depend on the result of threat analysis on the considered network product classes. In particular, the difference between tests that are considered to be part of security compliance testing or part of vulnerability testing is left for the normative phase. The details on the type of documentation that should be provided to vulnerability testers, in cases of white box testing, depends on the attacker model and is also left for the normative phase.

- 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 requires formal demonstration.

Having multiple assurance levels would:

- Make evaluators accreditation process more complex (different evaluators might not be able to go to the same level of depth or to apply the same rigour)

- Fragment the evaluation market as operators might request different assurance level for the evaluation of the same network product from a given vendor

- This would destroy the purpose of standardization effort which aims, amongst others, at reducing the cost and the number of evaluation by agreeing on a common acceptable level of assurance in a standard body for the entire industry

- This would also make results more difficult to compare for operators which might receive evaluation at different assurance level for two network product of the same network product class.

Considering that the three parameters are expected to be constant and the above mentioned additional complexity of having several assurance levels. 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.

4.5.2.3 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.

As pointed out in clause 4.3.1 "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 will be accomplished in the normative stage of SECAM during the SAS writing phase and be related to the threat and risk analysis outcomes.

At the end of this process, for each network product class, 3GPP SA3 will have precisely defined the attacker model as well as the operational environment assumption and the security requirements to mitigate the identified risks.
The expected modularity of SAS as described in clause 4.1.4 should allow an easy composition of SAS 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 will be built to achieve a security baseline deemed relevant by SA3 for a network product class. This will result in one security level per network product class (security level MME, security level HSS, security level eNodeB ...).
These baselines are not meant to be compared to one another as they are applying on different network product classes.

Having multiple security baselines for a single network product class would:

- Make evaluators accreditation process more complex (different evaluators might not be able to undergo the full range of security test of a given security baseline)

- Fragment the evaluation market as operators might request different security baselines for the evaluation of the same network product from a given vendor

    - This would destroy the purpose of standardization effort which aims, amongst others, at reducing the cost and the number of evaluation by agreeing on a common acceptable security baseline in a standard body for the entire industry

    - This would also make results more difficult to compare for operators which might receive evaluation against two different baselines for two network products of the same network product class.

- For a given network product class, operators might be willing to have an homogeneous set of equipment even if these equipment are deployed in various environments with different exposure levels. An average agreeable level will have to be found in the standardization process to make the evaluation practical. If some supplementary very high security requirements are required by a single or a few operators, these operators remain free to undergo further evaluations outside of the standard SECAM process.

NOTE: Alternatively, but in rare cases, if no satisfactory average can be found, you 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.

4.5.3 Roles

4.5.3.1 Roles involved in the security assurance process

Any security assurance process includes a number of roles. Figure 4.5.3.1-1 depicts the security assurance process studied in this technical report and indicates which roles are involved in it. New roles need to be defined in addition to the existing ones.

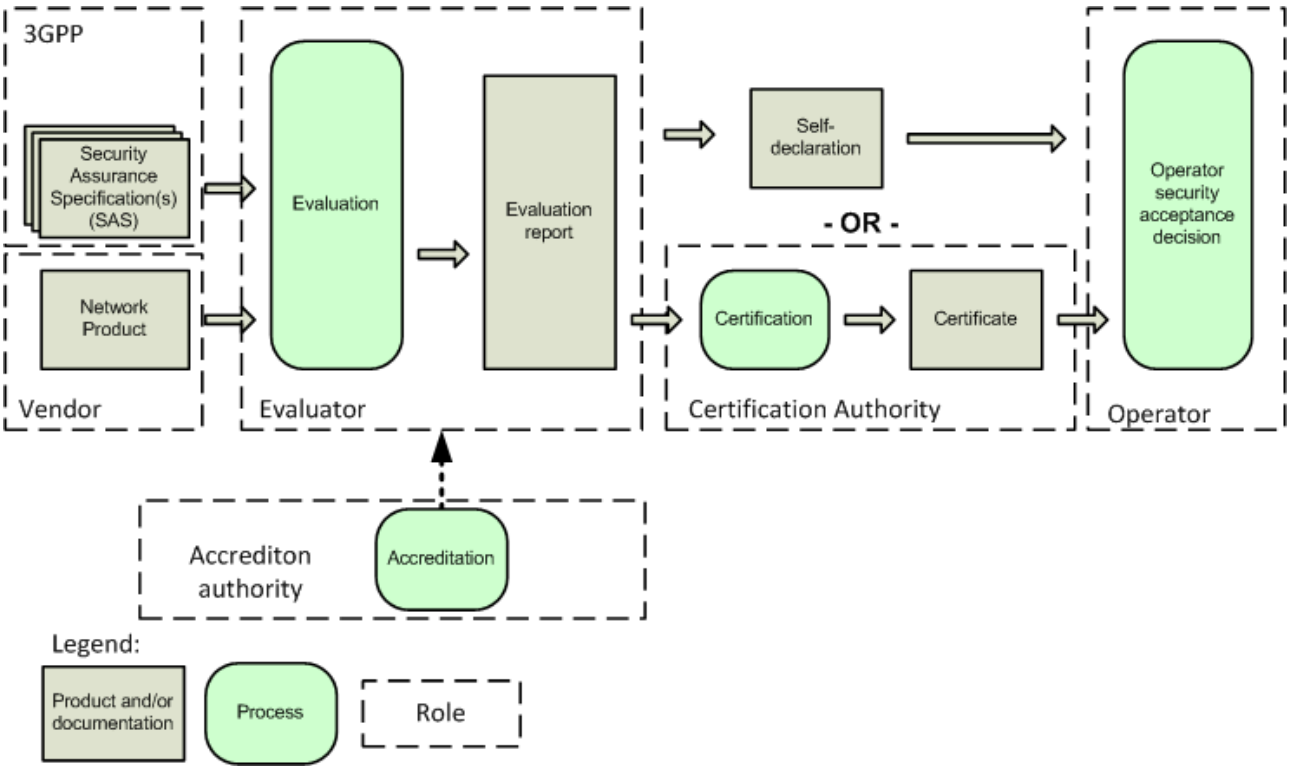


Figure 4.5.3.1-1 Roles involved in the security assurance process. The text "- OR -" in the figure indicates that the evaluation report may be provided directly to the operator or that it may be subject to certification first.

Figure 4.5.3.1-1 Roles involved in the security assurance process. The text "- OR -" in the figure indicates that the evaluation report may be provided directly to the operator or that it may be subject to certification first.

4.5.3.2 Implicit and existing roles

As explained in the introduction in clause 4.5.1, some roles are implicit from the existing business environment. These roles are the following:

- **Vendor** produces the network product;
- **Operator** makes the decision regarding accepting assurance of security properties of the product;
- **3GPP** is responsible for producing Security Assurance Specifications (SASs).

4.5.3.3 New roles

In addition to the already existing roles, three new roles are defined:

- Evaluator;
- Certification Authority;

- Accreditation Authority.

The definition of these roles is in clause 3.1. Unlike the implicit roles, the new role definitions do not fix which party should take on the role. For example, the vendor, the operator, a second or third-party, could take the evaluator role. If the vendor takes on the evaluator role it is referred to as self-evaluation. If certification is not use, the vendor provides a self-declaration to the operator.

3GPP does not have mandate to require that a certain role must be instantiated by a certain legal entity; only a regulatory body can effectively make such a requirement. 3GPP can however define the processes and roles and make an agreement on which party should take on the roles. This does not rule out that there will be regulatory requirements on who should take on a role that differs from the 3GPP agreement.

NOTE: The instantiation of these roles will be provided in the candidate methodologies if appropriate.

4.5.4 Sub-processes and documentation

4.5.4.1 Security Assurance Specification (SAS)

The Security Assurance Specification (SAS) for a given network product class provides a description of the security requirements 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.

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 SAS 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 5.2.2.1) is outside of the scope of this study.

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 [20]) or other publications.

NOTE 3: This clause needs to be further elaborated in the candidate methodologies.

4.5.4.2 Network product

The network product has to be accompanied by documentation regarding its development to facilitate proper evaluation. It can also be expected that the evaluator has to inquire further information from the vendor to perform the evaluation.

NOTE: This clause needs to be further elaborated in the candidate methodologies.

4.5.4.3 Evaluation and evaluation report

The evaluation results in an evaluation report that describes the evaluation performed and whether the evaluator deems that the network product fulfils the Security Assurance Specification(s) that it claims to fulfil.

NOTE: This clause needs to be further elaborated in the candidate methodologies.

4.5.4.4 Certification and certificate

If the evaluation report states that the network product passed the evaluation successfully, a Certification Authority may review the evaluation report. If the review concludes that the evaluation report is satisfactory, the Certification Authority may issue a certificate for the network product.

None of both candidate methodologies describes the certification process of a network product so far. Methodology 2 describes a process of vendor accreditation and a dispute process where the certificates are associated to vendors and not to products. Methodology 1 has well-understood provision for providing product certificate and network product certification. It should be possible for methodology 2 too if it is desired.

NOTE: This clause needs to be further elaborated in the candidate methodologies if appropriate.

4.5.4.5 Operator security acceptance decision

The operator examines the network product, the evaluation report (and possibly the certificate) and decides if the security assurance level is sufficient.

NOTE: This clause needs to be further elaborated in the candidate methodologies.

4.5.4.6 Revocation and dispute process

In the case 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), it is desirable that the candidate methodologies provide provision for conflict resolution and revocation.

NOTE: This clause needs to be further elaborated in the candidate methodologies if appropriate.

5 Proposed methodologies

NOTE: Every proposed methodology will have to provide a reasonable number of examples on how concrete security requirements can be described and tested with the regard to the sample network product classes of clause 4.2. These examples will be developed in Annex A for all proposed methodologies. Each methodology can use its own list of requirements.

5.1 Methodology 1: Common Criteria (CC)

Editor's Note: The CC Management Board (CCMB) and the CC Development Board (CCDB) have launched the update of the CCRA with new rules for the mutual recognition of certificates across national certification schemes. Applicability of these evolutions is FFS.

5.1.1 Introduction

The CC framework can be used as a model outside of the CCRA and this is what methodology 1 intends to do.
The roles used in this methodology are compliant with the roles defined in clause 4.5.

Editor's note: The concrete role instantiation for Methodology 1 is FFS.

Editor's note: Methodology 1 needs to clarify how the generic process of clause 4.5 (actors and roles) is meant to be implemented.

Editor's note: Methodology 1 needs to provide actionable details on which part of the CC framework should be kept and for which activity of SECAM.

Editor's Note: The terminology used in all of clause 5.1 needs to be harmonized. For example, the term "evaluation activity" and "evaluation techniques" must be defined and used consistently.

This methodology is based on the well-established practice for specifying and providing security assurance that has evolved over more than 20 years of scrutiny from many of the best security assurance professionals.

The Common Criteria ISO/IEC 15408 [15] provides three different aspects:

- It provides a common structure and language for expressing product security requirements (CC Part 1), a catalogues of standardized security requirement components and packages (CC Part 2 and 3)
- It provides the concepts of Protection Profiles (security requirements for network product classes) and Security Targets (security requirements for network products that may or may not claim compliance to certain Protection Profiles.
- It also provides the methodology and framework (CC Part 3) for the evaluation of products against known and understood requirements to gain confidence in the effectiveness of the security measures.

Editor's note: Methodology 1 needs to explain how the operator gets assurance of correct product implementation. E.g. through accreditation of the development process or product certification.

Unlike its early predecessors such as TCSEC that specified the requirements for a certain type of products, the CC framework is intentionally flexible, allowing the evaluation of products with a wide range of security properties, using different assurance methods. Over the years this has allowed the CC framework to be used for many types of products and environments.

This flexibility also means that a security evaluation may be performed with almost any product scope and for any type of security functionality. This flexibility means that a security evaluation (and certification) may have a very different content and qualities depending on the actual scope and security requirements applied for a specific product evaluation. Therefore the use of Protection Profiles is a way to ensure that different network products will be assessed with at least a certain scope, security functionality and security assurance requirements that is applicable to the network product class to which the network product belong. It is good way to utilise and control this flexibility that the CC framework gives us.

Below is a short description of the CC model, such the assurance model. This description is to large extent extracted from the Common Criteria [15] and adapted for the present document.

5.1.1.2 Assurance paradigm

Necessary for the discussion of the benefits and using the Common Criteria model is to understand the philosophy that underpins the CC approach to assurance. An understanding of this will permit the reader to understand the rationale behind the assurance requirements to better apply the CC model.

Critical for the understanding of the CC model is the concept of the Target Of Evaluation (TOE).
The TOE is the scope of the assessment (Target Of Evaluation) that will provide security functionality.

Editor's Note: More details about the definition of the TOE needs to be supplied.

The CC philosophy is that the threats to security and organisational security policies (i.e. policy requirements) should be clearly articulated. These will be translated into security objectives for the TOE and the TOE environment, such as the TOE together with the TOE environment must be able to address all the threats and organisational security policies. The TOE should then provide the security measures called TSF (i.e. TOE Security Functions) and they must be demonstrably sufficient to for their intended purpose, i.e. to satisfy the TOE security objectives and thereby (together with the TOE environment) to address all the threats and organisational security policies.

NOTE: For each TOE a preliminary threats analysis will be conducted. This threat analysis will also take in to consideration the environment where the TOE is deployed. The result of this threat analysis will be the security requirements to select between all the ones listed by Protection Profile (PP) or to add in a specific Security Target (ST). More details in clause 5.1.3.1.

5.1.1.3 Assurance approach

The CC philosophy is to gaining assurance based upon an evaluation of the product that is to be trusted. Evaluation has been the traditional means of providing assurance and is the basis for prior evaluation criteria documents. In aligning the existing approaches, the CC adopts the same philosophy. The CC proposes measuring the validity of the documentation and of the resulting product by expert evaluators with increasing emphasis on scope, depth, and rigour.

Editor's Note: It needs to be clarified what documentation is intended and how the expertise of the evaluator is ensured.

The CC framework does not exclude, nor does it comment upon, the relative merits of other means of gaining assurance than the one described in CC Part 3 [15]. Research continues with respect to alternative ways of gaining assurance. As mature alternative approaches emerge from these research activities, they will be considered for inclusion in the CC, which allows the new measures for gaining assurance to be used by the evaluators.

Assurance can be derived in many different ways. However, the CC framework provides assurance through active investigation. Active investigation is an evaluation of the product in order to determine its security properties.

Editor's note: More clarification on these active investigation activities is needed.

One of the main purposes of the evaluation is therefore to active search for potential vulnerabilities. This is done with the evaluation techniques detailed in clause 5.1.4 such as the evaluation for the correctness of the implementation of the network product.

Evaluation techniques can include, but are not limited to analysis of development processes and procedures; analysis of design documentation; analysis of guidance; analysis of develop testing; independent testing; vulnerability analysis and penetration testing.

Unlike safety and quality control, the evaluation of the network product is a means to gain assurance that the product is able to withstand accidental threats (e.g., badly configured password policies) as well as intentional attacks performed by hostile attackers.

The prime factor to consider when establishing confidence in security countermeasures is trust in the source of the countermeasure. Therefore particular attention shall be paid to the selection of the vendor or any other entities involved in the development of the product.

5.1.1.4 CC evaluation assurance scale

A core part of the CC philosophy is that greater evaluation effort results in greater assurance. Another core part is that minimal effort should be applied to provide the necessary level of assurance. The increasing level of effort is based upon:

a) scope – that is, the effort is greater because of a larger scope of the evaluation aspects and evidence of the product is included;

b) depth – that is, the effort is greater because it is deployed to a finer level of design and implementation detail;

c) rigour – that is, the effort is greater because it is applied in a more structured, formal manner.

The CC defines seven different assurance levels. The Evaluation Assurance Levels (EALs) provide an increasing scale that balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance. Although the assurance requirements in CC part 3 are described one by one, they are in most cases referred to as the package defined in an EAL. There is nothing preventing authors of PPs or STs to add existing CC Part 3 requirements to an EAL (this is called augmentation) or to add new PP or ST specific assurance requirements (this is called extended).

In many cases, in a Protection Profile (PP), existing assurance requirements from CC part 3 are simply refined with additional detail on how testing or vulnerability analysis should be performed, or what is required from the design documentation (in addition to what CC requires). This is a good way for the PP writer to be more specific.
The refinements are considered to be valid refinements as long as the existing assurance requirement has not been weakened.

5.1.1.5 CC assurance and the significance of vulnerabilities

It is assumed that there are threat agents that will actively seek to exploit opportunities to violate the security objectives both for illicit gains and for well-intentioned, but nonetheless insecure actions. Threat agents may also accidentally trigger security vulnerabilities, causing harm to the organisation. Security breaches arise through the intentional exploitation or the unintentional triggering of vulnerabilities in the use of the product.

Vulnerabilities can arise through failures in:

a) requirements – that is, an product may possess all the functions and features required of it and still contain vulnerabilities that render it unsuitable or ineffective with respect to security;

b) development – that is, an product does not meet its specifications and/or vulnerabilities have been introduced as a result of poor development standards or incorrect design choices;

c) operation – that is, an product has been constructed correctly to a correct specification but vulnerabilities have been introduced as a result of inadequate controls upon the operation.

Assurance is grounds for confidence that a network product meets its security objectives (which were determined when the SAS was written). This means that the product provides the security functionality in such a way that they are correct (as described) and effective (meet their purpose).

The vulnerability assessment activity (see clause 5.1.4) covers various vulnerabilities that may be present in the development and operation of the network product. This does not mean that the vulnerability assessment is a continuous activity performed during the development or the operation. Development vulnerabilities take advantage of some property of the product, which was introduced during its development, e.g. defeating the self-protection through tampering or defeating non-bypassability by circumventing (bypassing) the security functions.
Operational vulnerabilities take advantage of weaknesses in non-technical countermeasures to violate the security objectives, e.g. misuse or incorrect configuration. Misuse investigates whether the product can be configured or used in a manner that is insecure, but that an administrator or user of the product would reasonably believe to be secure.

One of the main purposes of the evaluation is therefore to active search for potential vulnerabilities.

This means that during all evaluation activities, using the information the evaluator has to gain experience and understanding of the product, and actively search for potential vulnerabilities (against the security objectives) that may exist in the intended operation environment of the product. In a separate vulnerability analysis activity the evaluator will try to identify additional potential vulnerabilities and finally also assess whether or not any of these potential

vulnerabilities can be exploitable in the intended operational environment. Some of the vulnerabilities may not be exploitable at all, while other may be exploitable only with certain effort (attack potential).

For a product to pass the evaluation there must be no known exploitable vulnerabilities that can have a significant impact in the 3GPP context. This means that the attack potential must be known and part of the intended operational environment.

There are several factors determining the quality of the vulnerability analysis. First, the ability to find vulnerabilities depends on the availability of information of the product and its development environment (e.g. design information, source code, delivery process, etc.). Second, the rigour and formalism of the vulnerability analysis is also relevant to the ability to find vulnerabilities. Third, each vulnerability has to be judged against an attack potential to determine which of the vulnerabilities may be considered exploitable and which may be considered residual (i.e. exploitable only with an increased attack potential). These factors are determined by the Evaluation Assurance Level (EAL).

5.1.1.6 Concept of ST and PP

Since the CC framework in itself never indicates which security requirements a certain security product or types of products shall meet, this has to be specified. The Security Assurance Specification (SAS) may specify any scope, any Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) (see further clause 5.1.3.1). The CC framework requires that the security specification follows a standardized format in order to:

- ensure that specific content needed to assess a product against the security specification is available;
- allow comparison of ST of different products.

There are two types of specifications in CC: Protection Profiles (PPs) and Security Targets (STs). The PP is the specification for a certain type of product while the ST is the security specification for a specific product. Such as there might be a PP for firewalls and a ST for Firewall XYZ. The ST for the Firewall may claim compliance with the firewall PP. There may be different PPs for different types of products or properties and one ST for a product may claim compliance with none, one or multiple PPs.

The advantage of this is that it is possible to specify only the minimum requirements in one PP for a certain type of products in one document, without having to provide more details than necessary. At the same time it is possible to ensure that vendors can claim compliance with the PP and also ensure that the ST provides the additional informational to make it into a complete ST.

This means that a PP is less complete than an ST and has less detailed information than an ST. The PP will never describe an implementation, but a PP author may want to give more or less freedom to the implementation of the security functionality. An ST may also extend the requirements beyond the requirements in the PP.

The CC provides a catalogue of Security Functional Requirements (SFRs) and the Security Assurance Requirements (SARs) in CC Part 2 and Part 3. The PP and ST writers may use these catalogues to select the requirements for the PP and ST, but may also define their own. However, it is not only very useful to rely on the catalogue of SFRs since readers of STs will be familiar with these SFRs. The CC also requires that new SFR should only be introduced if the available SFR from CC Part 2 are not sufficient. There is also much experience and know-how that has gone into these requirements. Still it is up the ST and PP writer to select and instantiate (complete) the SFRs that are provided in CC Part 2.

Since both the PP and the ST are formal documents there are several different guides available how to write these documents. In addition to the CC Part 1, different guides are available. One example is the ISO/IEC TR 15446 "Guide for the production of Protection Profiles and Security Targets".

5.1.1.7 Specific issues on Protection Profiles (PPs) and Security Targets (STs)

An ST is the security specification for a specific network product. The ST is produced by the vendor and describes how the network product implements security measures to fulfil the security requirements in the ST. The evaluator performs an evaluation during which the evaluator determines whether the network product fulfils the security requirements in the ST with the security assurance level prescribed by the Security Assurance Requirements (SARs) in the ST.

The ST is compliant with a PP if the requirements in the ST are as strict as or stricter than in the PP.

There are also requirements on PPs and STs. A PP must be complete, consistent and technically sound and suitable for use as a template on which to build another PP or an ST. In a similar way an ST must be complete, consistent and

technically sound and suitable for use as a basis for a TOE evaluation. This is determined by the evaluation of PPs and STs. PP can be evaluated and certified independent of any product, while the ST evaluation is only performed as the first step in any TOE evaluation.

These strict requirements on PPs and STs will ensure the quality and consistency. It has the benefit that unnecessary nice-to-have requirements that do not really provide any increase in security can be easily avoided since there must be a security objective behind all security requirements. Having security requirements not relating to security objectives is less likely to happen. The security objectives also require the appropriate threats or organisational security policies. Also the PP and the ST are mainly concerned with the TOE. Any parts that are outside of the TOE, i.e. the TOE environment, are not subject to the same assessment. The development environment is addressed by the Assurance measures for Life-Cycle (ALC) and the operational environment is addressed by the guidance (AGD). Still they are considered in the vulnerability analysis.

5.1.2 Content of a Security Assurance Specification (SAS)

5.1.2.1 Overview of SAS

The purpose of a SAS is to specify the overall security requirements for network product classes. There will be one SAS for each network product class. An SAS will consist of three different parts covering different aspects:

- A Protection Profile (PP), which specifies the scope of the Target Of Evaluation (TOE), the security functional requirements and the assurance requirements.
- Software hardening requirement (e.g., disabling or removing unused network services).
- Hardware hardening requirements (e.g., disabling or removing unused external ports).

The first part is covering the TOE, which means that should cover the security functions of the network product class. The software and hardening requirements are primarily to remove or reduce the attack surface of the network product. Just as for the PP vs. ST relationship, the hardening requirements consist of generic security objectives as well as instantiated requirements.

NOTE 1: The split of documents between PP and hardening guidelines in methodology 1 is made for documentation reasons and does not put weight on this specific assurance activity.

Editor's note: The templates to use for these requirements are FFS.

Editor's note: The intention is to cover these hardening guidelines with refinements of the AGD_PRE component. The concrete refinements of AGD_PRE for this purpose are FFS.

Editor's note: Clarification on the scope of application on this software and hardware hardening requirements and guidelines is FFS.

Editor's note: Concrete examples of hardening guidelines and their evaluation are FFS.

The difference between the PP and the hardening requirements for software and hardware may be illustrated as in the picture below.

Editor's note: in general the actors (e.g. evaluators vs. auditee, vendors vs. third-party labs) and the phases in this methodology are FFS; consequently who will assess compliance of OS/hardware against OS/hardware hardening guidelines FFS.

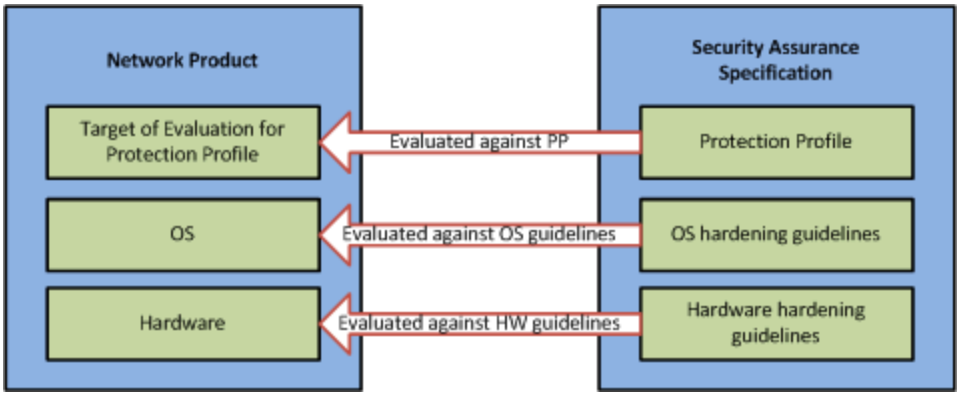


Figure 5.1.2.1-1 Network product class and the security requirements

The software hardening guides may not limited to operating systems or COTS products. Depending on the scope of the TOE it cannot be excluded that some parts of the TOE that will be covered by hardening guides. However, the hardening guides are addressing potential attack surfaces provided by these parts and not any security functionality provided.

NOTE 2: The distinction between the software and hardware hardening guides is not that they are restricted to hardware or software measures, but that they are related to the hardware interfaces and software interfaces. This means that deactivating a hardware interface may fulfil software hardening requirements and vice versa.

Although, it is possible to have to have all SAS requirements for a certain network product class in one document, it may is also possible to have each part in separate documents. By having separate documents it is easier to build modular SASs. Below is a description of each part.

Editor's note: It is important for the methodology how the information is portioned in one or more documents. The best way to do it can be resolved once SA3 has decided on a methodology.

NOTE 3: The assumption is that hardening guidelines are being verified.

5.1.2.2 Description of the Protection Profile (PP) part

The concept of Protection Profiles was first developed with the Federal Criteria in 1992. Since then it has been evolved with the Common Criteria and the latest revision CC3.1R4 [15] is specifying the requited structure and content in Part 1, Appendix B.

By following the standard and the latest version of the standard, it is possible to take advantage of the on-going development of the standard. It specifies the following clause of a PP:

1. PP introduction – Providing a narrative description of the product type and its intended use, the scope of the TOE and its major security features.

2. Conformance claims – Stating whether the PP claims conformance to any specific version of the CC, any specific PPs and/or packages (such as a specific EAL).

3. Security problem definition – Identifying the threats, Organisational Security Policies (OSPs) and assumptions that are relevant to the TOE.

4. Security objectives – Specifying how the security problem is addressed by a division between security objectives for the TOE and security objectives for the operational environment of the TOE.

5. Extended components definition – The definition of any extended functional and assurance requirements, beyond the ones defined in CC Part 2 or CC Part 3.

6. Security requirements – The applicable security requirements for the TOE, i.e. the functional requirements as well as assurance requirements are given here in this clause. They are the requirements that are necessary to meet the security objectives for the TOE. These security requirements are using a common and well-defined structure and language. These security requirements may contain adaptions such as instantiations and refinement of the requirements provided in the CC Part 2 and CC Part 3, as well as the extended requirements in clause 5.

The most interesting part for 3GPP is probably clause 1, clause 3 and clause 6.

Clause 1 has to specify the network product class, the scope of the TOE, summarise the security features, as well as the intended use. This clause is essential for the rest of the PP.

Clause 3 defines the consensus of 3GPP regarding the assets to be protected, the considered threats and the consensus on environment assumptions. It implicitly relies on a further consensus regarding the attack paths that could be used by an attacker to compromise assets on the TOE. All these elements have to be defined within 3GPP before a PP can be defined.

Clause 6 specifies the security requirements. Although the generic functional requirements may be taken from CC Part 2 or may be defined in clause 5, they have to be instantiated and refined, at least to the extent that they are meaningful to fulfil and still remain applicable to all network products of the network product class.

3GPP could also have to clarify interpretation of requirements, e.g. in a supporting document. Such activities are typically performed to help vendors and evaluators to interpret Security Assurance Requirements (SARs) in a given context, but also could be used to clarify some generic SFRs, e.g. SFRs related to security policies in information flow control or security audit.

In the context of SECAM, it is not possible for vendors to add or remove in the ST any security features or additional information to be evaluated.

An example of audit generation FAU_GEN.1.1 taken from the OSPP v3.9 [16] and NDPP v1.1 [17]:

CC3.1R4 Part 2	FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events: Start-up and shutdown of the audit functions; All auditable events for the [selection, choose one of: *minimum, basic, detailed, not specified*] level of audit; and [assignment: *other specifically defined auditable events*].
OSPP v3.9	FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events: Start-up and shutdown of the audit functions; All auditable events for the **not specified** level of audit; and **all modifications to the set of events being audited;** **all user authentication attempts;** **all denied accesses to objects for which the access control policy defined in the OSPP base applies;** **explicit modifications of access rights to objects covered by the access control policies; and** **other specifically defined auditable events as defined in the table in FAU_GEN.1.2.**
NDPP v1.1	FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events: Start-up of the audit functions; All auditable events for the **not specified** level of audit; and **All administrative actions;** **Specifically defined auditable events listed in Table 1**. **Table 1 – Auditable events and audit record content:** **FIA_UIA_EXT.1 All use of the identification and authentication mechanism. (Provided user identity, origin of the attempt, e.g., IP address).** **FPT_STM.1 Changes to the time. (The old and new values for the time. Origin of the attempt, e.g., IP address).** […]

This means that the ST author may add additional auditable events to this list. This may even be necessary if additional security features are included.

The assurance requirements, unlike the Security Functional Requirements (SFRs), must not be refined. However, they can be refined by describing how a certain network product class shall be documented or its security functionality tested.

5.1.2.3 Hardening

Editor's note: Details on what are the input/output and actors involved in these hardening activities in the context of SECAM is FFS. Level of details of the hardenings guideline issued by these different actors is also FFS.

The purpose of hardening is to contribute to reduce the attack surface of the network product. This can be achieved by both software, and hardware and configuration methods. Examples of software methods are to remove unnecessary services and unused user accounts. An example of a hardware method is to physically remove unused USB ports. An example of a configuration method is to prevent the local access to an eNB.

Hardening is can be platform specific. For example hardening actions might differ somewhat between different types of operating systems. Further, hardware, operating systems and applications may be proprietary. This may or may not affect what a SAS list of concrete hardening actions can contain.

5.1.2.4 Description of the software hardening part

The whole principle of hardening is not (only) to remove services or features that are known to have vulnerabilities, but to identify and remove any services or features that are not necessary and to reduce the remaining services to the minimum required.

Software hardening is typically done for COTS products such as operating systems and applications that may be installed with a lot of services and features that are not necessary for the network product to run, and will provide an attack surface.

On a high level the software hardening is divided into the identification of unnecessary properties and features, and the elimination of them. For certain products there may exist hardening guides that will help with the elimination of them.

At the first level all external visible attack surface, functionality that is not necessary for the network product must be identified. This can be done by identifying services and processes, but also by testing which services are visible on the external interfaces. Privileged applications (e.g. set user-ID programs) are also considered to be potential risks and should be reduced to a minimum of necessary services. Also configuration files must be analysed to identify accounts, access rights and privileges and limited to the minimum required.

There are two ways to deal with unwanted services and features. The first and best is not to install them in the first place, since this will prevent them from being activated later, by mistake or by an insider. The second approach is to deactivate the service by changing the configuration. The second approach will only be effective if these services cannot be activated by unprivileged users or automatically, e.g. by restarting the system.

There is a third way to deal with unwanted services and features. This is to make assumption or restrictions in how the product is supposed to be used. This may include reducing the exposure to services by imposing firewalls or filtering mechanisms in the environment of the network product.

For systems that are under maintenance it has to be ensured that the hardening remains also after system maintenance or upgrade has been performed.

Editor's note: Clarification on the necessary adaptation on flaw remediation process in CC to support system maintenance or upgrade for hardware and software is FFS.

Experience has shown that upgrading or installation of applications may change the hardening. Installation or even the installation process for installing new applications may also require a deviation from the hardening. Sometimes maintenance may require more functionality or access rights to the users performing maintenance. All services interfaces are very good attack surface candidates.

5.1.2.5 Description of the hardware hardening part

Hardware hardening is on a high, principal level, very similar to software hardening. An attack surface is an attack surface independent of it is a hardware or software interface. However, a physical access may limit the possible attackers. Also the steps and security measures taken in hardening are different.

5.1.2.6 Definition of the expected environment of the network product class in the context of writing the 3GPP evaluation profile

There are certain aspects of the operational environment for a network product that are relevant for security.
The relevant aspects are divided into threats that have to be addressed (by the network product) and needs on the environment from the network product in order to effectively address these threats. These needs are formulated as assumption on the environment that has to be fulfilled. In addition to the threats the environment may have policies resulting in security requirements on the network product. These policies are called organisational security policies.
In addition to the threats there is also an assumed attack potential to an attacker behind the identified threats.

By having a well-defined description of the environment it will be possible to identify if there exist additional threats that are relevant, if there is an attack potential that is beyond the one assumed, or if it is not possible to meet the assumptions, i.e. to satisfy the need of the network product class.

5.1.3 Methodology for development of a SAS

5.1.3.1 Overview

One should not believe that a PP is enough to enable evaluation within 3GPP actors. It should be noted that many communities using CC evaluation as a standard also heavily rely to ad-hoc supporting documentation.

Example of this can be found in smartcard community, which had to issue

- specific guidelines refining almost all CC assurance components
- refinements on CEM, such as the application of "attack potential"
- etc.

Considering that at present time, many ITSEFs and local certification bodies do not have the required skills to assess specific notions or protocols used in the network products within the copse of SECAM, there is also a need for non-public shared documentation describing

- the expected skills of evaluators,
- the consensus on attacks paths and methods that should be verified during AVA_VAN evaluation,
- etc.

It is impossible to conclude that CC is cost effective without a complete list of the needed supporting documents.

Editor's note: The complete list of expected CC supporting document is FFS, as well as the description of the evaluation process (roles, actors, steps and so on).

Editor's note: There is a need for more explanation on the identification and mapping between the security threats, security objectives. Which parts of CC document provide this clarification and how to reuse it is FFS.

5.1.3.2 How to identify suitable SFRs and SARs for the PP

There are several good documents describing how to write Protection Profiles (and also Security Targets). First of all there is the ISO Technical Report ISO/IEC TR 15446:2009, but there are also different national documents describing this.

Although the methodology usually is presented as a top-down method, writing a PP is always an iterative process.
It is useful to start with a general problem description, written in natural language. This is usually more helpful than any formalism since it will establish a general understanding of the security problem and its solution before starting the more formal work.

The steps are following the structure of the clauses in the PP, but with iterations and repeated refinements.
The formal parts can be summarised in the following steps:

- threat analysis;
- the security problem is first defined based on the threat analysis;
- the security objectives are then identified to address the security problem;
- security requirements are then defined to satisfy the security objectives for the TOE;
- actual security functions are then selected to satisfy the security requirements.

Usually, an iterative process will be required. For example, definition of security requirements may highlight clarifications needed to the definition of the security objectives or even the security problem. In general, a number of iterations may be required in which the relationships between threats, organisational security policies, security objectives and security requirements and functions are examined closely, particularly when rationales are being constructed. Only when all identified gaps in the rationales are filled may it be assumed that the PP is complete.

5.1.3.3 How to help vendors and evaluators to use the PP

Editor's note: There is a need for further explanation and adaptation of CC for specific 3GPP context. In particular:

- What are the typical evidences one should use for design documentation? (ADV_*)
- What are the baseline methodological requirements for compliance tests (ATE)?
- What are the state-of-the-art vulnerability tests for AVA_VAN?
- What types of configuration and test beds are allowed for third-party test (ATE_IND) and AVA_VAN?
- What is the 3GPP understanding of user guidance? (e.g. will the hardening guidelines be part of user guidance?)

5.1.4 Evaluation of a network product against a SAS

Using the methodology provided with Common Criteria there are security assurance requirements, provided by CC Part 3 and packaged in evaluation assurance levels or explicitly stated requirements described by the PP (or even ST).

The security concept is the confidence in countermeasures, and that this confidence is achieved by evaluation (picture taken from CC Part 1)

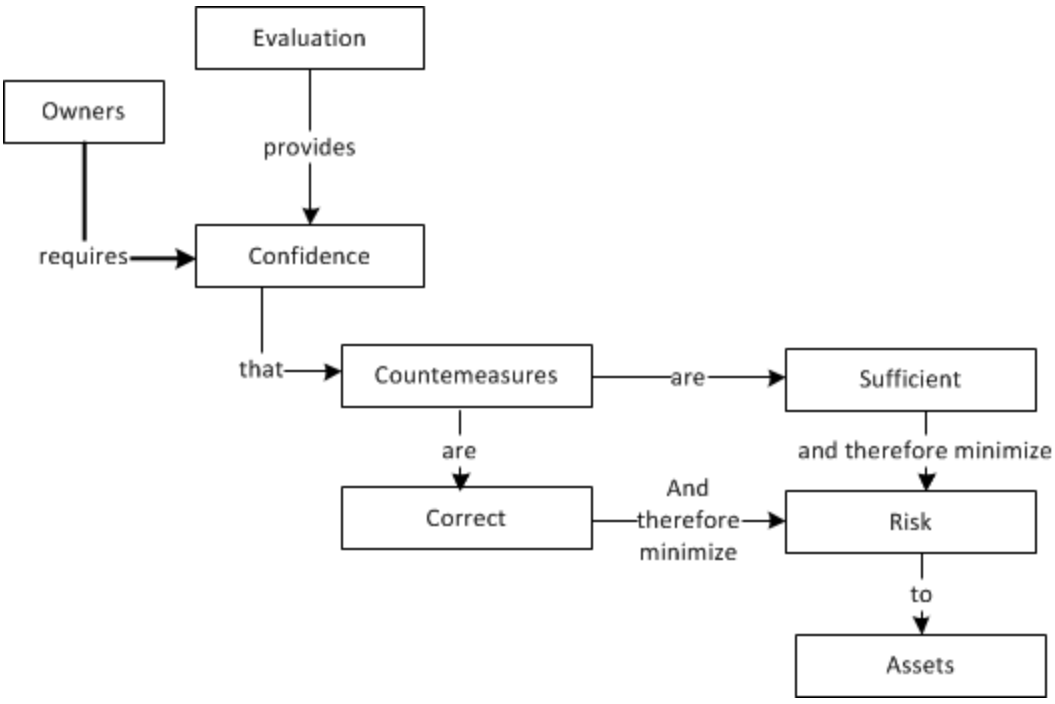


Figure 5.1.4-1: CC security concept

This assurance can be derived in many different ways. However, the CC provides assurance through active investigation of an evaluator. Active investigation is an evaluation of the IT product in order to verify that the countermeasures are correct and effective (sufficient). One of the main purposes of the evaluation is therefore to active search for potential vulnerabilities.

The evaluation techniques described by the CC include, but are not limited to:

a) analysis and checking of process(es) and procedure(s);

b) checking that process(es) and procedure(s) are being applied;

c) analysis of the correspondence between TOE design representations;

d) analysis of the TOE design representation against the requirements;

e) verification of proofs;

f) analysis of guidance documents;

g) analysis of functional tests developed and the results provided;

h) independent functional testing;

i) analysis for vulnerabilities (including flaw hypothesis);

j) penetration testing.

Editor's note: Providing an average level of assurance expected by methodology 1 for the above mentioned evaluation techniques in the context of SECAM is FFS.

Which of these evaluation techniques defined by 3GPP that should be applied and when, is determined by the assurance requirements. These assurance requirements specifies what the developer shall provide or do (D), the content and presentation of any provided documentation (C) and what the evaluator shall do to verify this (E).
E.g., development security (ALC_DVS) is concerned with the developer's physical, procedural, personnel, and other security measures. There are no ALC_DVS requirements for EAL1 and EAL2, ALC_DVS.1 (identification of security measures) is part of EAL3 to EAL5, while ALC_DVS.2 is for EAL6 and EAL7. Using at ALC_DVS.1 as an example:

- ALC_DVS.1.1D – The developer shall produce and provide development security documentation.
- ALC_DVS.1.1C – The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.
- ALC_DVS.1.1E – The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
- ALC_DVS.1.2E – The evaluator shall confirm that the security measures are being applied.

This means that security assurance measures specify **what** the developer has to provide and **what** evaluator shall do. The details **how** the evaluator shall do this and how to document this is documented in the CEM (the CC Evaluation Methodology). CEM identifies work units for the evaluator. This means that for ALC_DVS.1 there are the following work units described in CEM:

- ALC_DVS.1-1 The evaluator shall examine the development security documentation to determine that it details all security measures used in the development environment that are necessary to protect the confidentiality and integrity of the TOE design and implementation. (Related to ALC_DVS.1.1E)
- ALC_DVS.1-2 The evaluator shall examine the development confidentiality and integrity policies in order to determine the sufficiency of the security measures employed. (Related to ALC_DVS.1.1E)
- ALC_DVS.1-3 The evaluator shall examine the development security documentation and associated evidence to determine that the security measures are being applied. (Related to ALC_DVS.1.2E)

These assurance requirements may be extended or refined as is happening in the NIAP PPs by providing more details in the assurance measures. E.g., it is possible to change ALC_DVS.1.1C to require specific information to be covered by the security documentation, such as requirement on having an alarm system, doing background check of developers, etc. If there are completely new assurance requirements developed, there is also a need for providing the equivalent CEM information for how these requirements shall be verified.

5.2 Methodology 2

5.2.1 Overview

Each 3GPP network product class listed in clause 4.4 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. This methodology assumes the 3GPP network product classes listed in clause 4.4 as the targets.

Each 3GPP network product, within a network product class, is basically a device composed of hardware (e.g. chip, processors, RAM, network cards) and software (e.g. operating system, drivers, applications, services, protocols); in addition the 3GPP network product can 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.

A pre-requisite for the SAS writing part of methodology 2 is to have a complete list of features/capabilities considered relevant by SA3 for evaluation. The final list of features/capabilities and consequently the list of security requirements will depend on the results of a threat analysis done in the normative phase of this study.

SECAM evaluation will cover the following four 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 Security Assurance Process)
- Security Compliance Testing (assessing if requested security requirements are correctly implemented in a network product)
- Basic Vulnerability Testing (running of a set of FOSS/COTS tools on external interfaces of the Network product)
- Enhanced Vulnerability Analysis (holistic approach to analyse risk and impact of Vulnerabilities found in the Network Product))

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

Table 1 Mapping between SECAM phases and involved party.

SECAM tasks	Accredited actor
Vendor network product development and network product lifecycle management process assurance compliance	Accredited vendor
Security compliance testing	Accredited vendor or accredited third-party evaluator
Basic Vulnerability Testing	Accredited vendor or accredited third-party evaluator
Enhanced Vulnerability Analysis	Accredited vendor or accredited third-party evaluator

Consequently, according to table 1, SECAM can take many forms, depending on who performs security compliance testing, who performs Basic Vulnerability Testing and who performs Enhanced Vulnerability Analysis (EVA). SECAM is intended to enable self-evaluation where the vendors evaluate their network products if they have the proper accreditation for that. Methodology 2 provides all provisions for this need.

In Methodology 2 the responsibility for writing and managing the accreditation and monitoring rules is taken by a SECAM Accreditation Body. SECAM Accreditation Body's role also includes the handling of the dispute process. Methodology 2 will propose GSMA for taking this role and will provide a clear delineation between SECAM work in 3GPP and SECAM-related work in GSMA.

Even if it describes the complete process, including evaluation by accredited actors under SECAM Accreditation Body control and Security Assurance Specifications (SAS) writing, Methodology 2 does not prevent that 3GPP SAS security requirements and tests cases are used directly by mutual consent between vendors and operators without the accreditation process in place if wished so. 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 conflict 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.

Accreditation is intended to be valid for a limited time period and repeated at a frequency defined by the SECAM Accreditation Body (see clause 5.2.3 for details).

The ultimate output of the SECAM process is:

- an evaluation report proving compliance of a 3GPP network product with the 3GPP security assurance specifications
- optionally a certificate proving the accreditation of actors performing the evaluation tasks

An evaluation report will be issued for each 3GPP network product evaluated, and an optional certificate will be maintained for each actor.

The operator examines the network product, the compliance reports and the testing laboratories certificate published by the SECAM Accreditation Body and decides if the results are sufficient according to its internal policies (see 5.2.6 for details on Operators' security acceptance decision).

Below are several examples of instantiation of roles for SECAM:

Example 1: Combination of self-evaluation (for security compliance) and third-party evaluation (for basic vulnerability testing and enhanced vulnerability analysis) for the evaluation of a 3GPP network product (e.g. MME A of vendor X)

In the example below:

- Vendor development process assurance compliance is self-assessed by a vendor, which has previously been accredited by the SECAM Accreditation Body for this task. This assessment covers Life cycle management of the network product (e.g. control of update in development …). More details on these aspects are in clause 5.2.2.3.
- Security compliance testing is self-assessed by a vendor, which has previously been accredited by the SECAM Accreditation Body for this task;
- Basic Vulnerability Testing is self-assessed by a vendor, which has previously been accredited by the SECAM Accreditation Body for this task;
- Enhanced Vulnerability Analysis is assessed by an accredited third-party laboratory which has previously been accredited by the SECAM Accreditation Body for this task.
- The operators, and the vendors as far as third parties are concerned, receive the report from all four tasks of the evaluation and the vendor's self-declaration for a given network product and are able to check that all involved parties (self-evaluating vendors and/or 3rd party evaluators) were accredited to undertake the tests by checking their accreditation with the SECAM Accreditation Body.

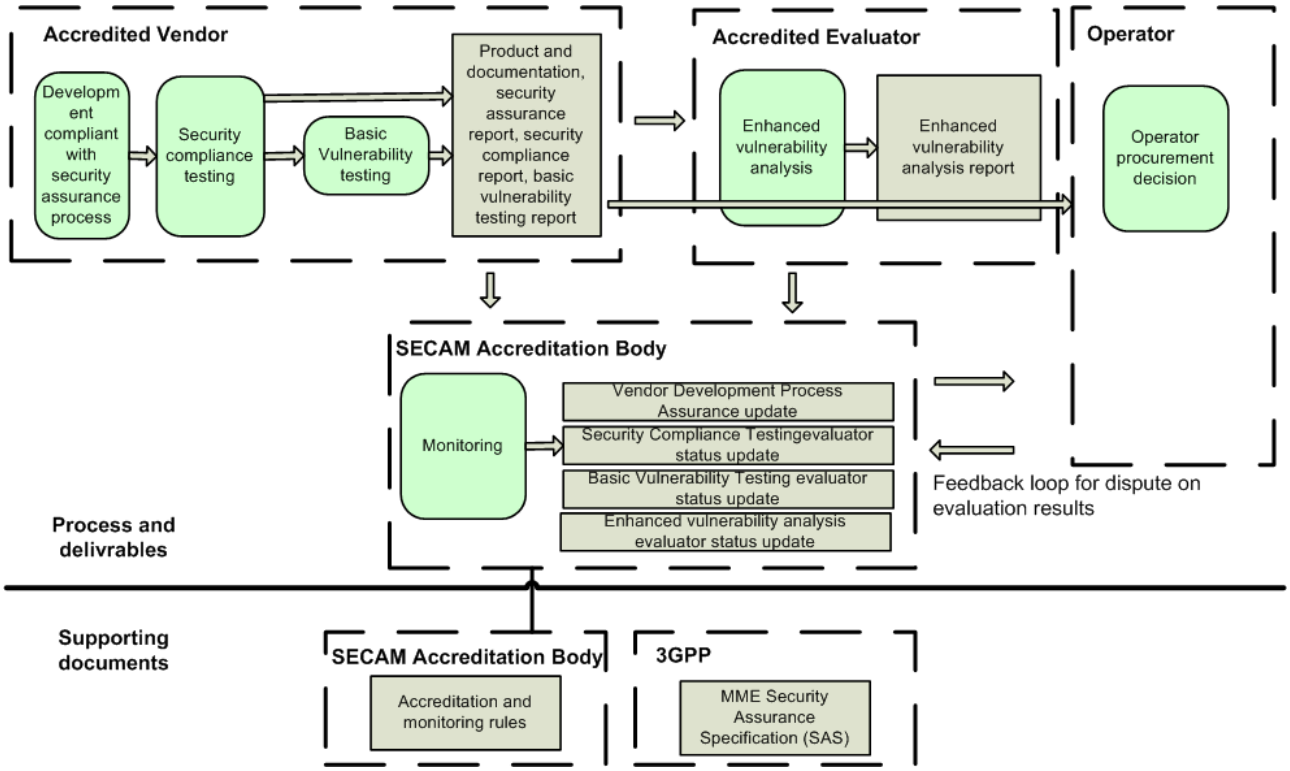


Figure 5.2.1-1: Combination of self-evaluation for security compliance and basic vulnerability testing and third-party evaluation for Enhanced Vulnerability Analysis for the evaluation of a 3GPP network product (e.g. MME A of vendor X)

Example 2: 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 is also accredited to undertake Enhanced Vulnerability Analysis and thus conduct all the three phases of evaluation.

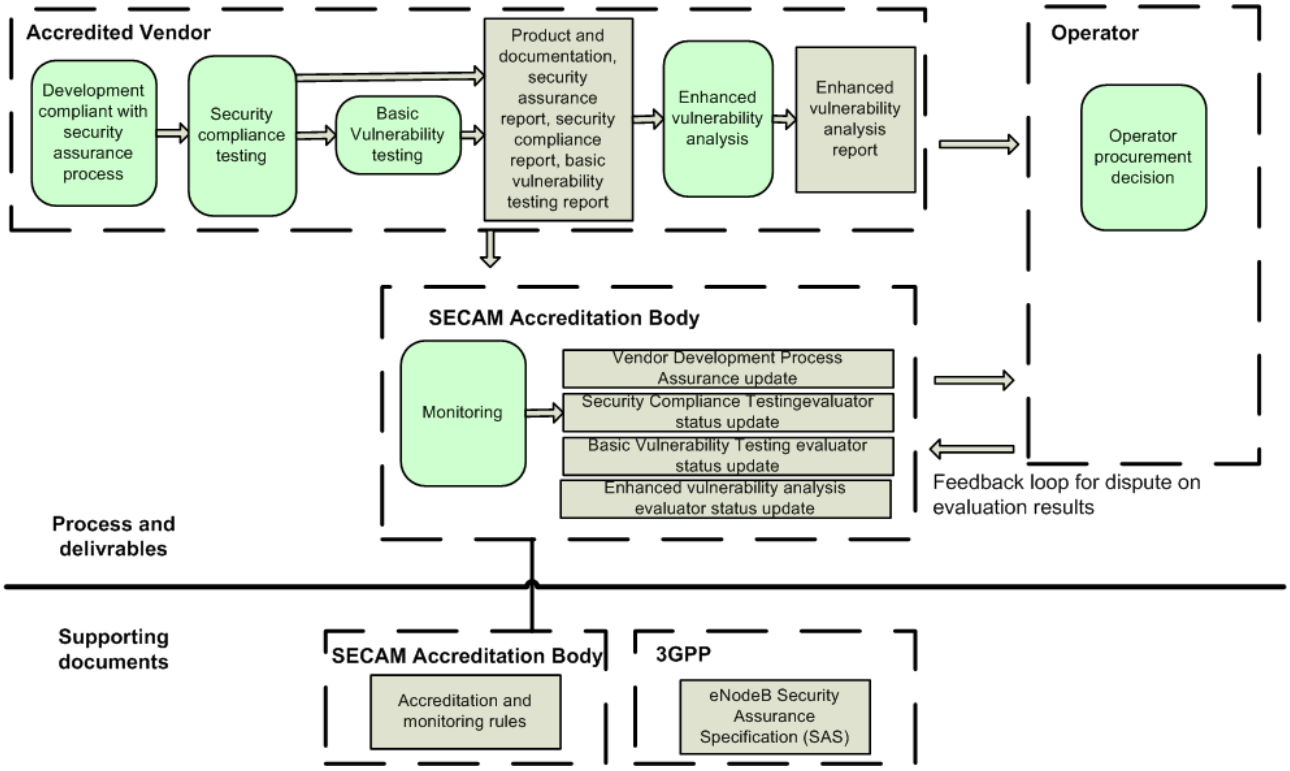


Figure 5.2.1-2: Complete self-evaluation of a 3GPP network product (e.g. eNodeB B from vendor Y)

Evaluation results check by the operators and dispute

The operator does not need to be accredited to perform again the tests made by the evaluators 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 operators complaint might be useful. This description will be part of the description of the complete dispute resolution process is likely to be left to the SECAM Accreditation Body and will be outside of the scope of 3GPP. For more details see clause 5.2.7.2.

5.2.2 Methodology building

5.2.2.1 Overview

SECAM methodology building is described in figure 5.2.2.1-1 hereafter. First, 3GPP will undertake a threat analysis and then will derive the SAS for each identified network product class as well as one security assurance process document. The security assurance process document will describe the whole security assurance process (evaluation, relation to accreditation body, general description of desired assurance level …).

Editor's note: Clarification on how these documents will be mapped to 3gpp documents (TS, TR 33.9bb – Technical Reports intended for publication …) is FFS.

The SAS will contain the detailed security requirements identified by SA3 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.

NOTE 1: The security requirements contained in an SAS are security functional requirements in the sense of Common Criteria [15], or hardening requirements. Security assurance requirements in the sense of Common Criteria [15] are embodied in the test cases and test results of an SAS.
There are no other security assurance requirements in an SAS, apart from the test cases and test results, and, hence, there is no separate testing against any security assurance requirements when testing for compliance with an SAS.
There are, however, tests against Vendor Development process assurance requirements, cf. clause 5.2.2.3.

NOTE 2: The number of documents to be delivered by SA3 will depend on the grouping chosen for the SAS.

The definition of the security requirements to use during the security compliance task will be conducted during the normative phase. The definition of the requirements to use for the Basic vulnerability testing and Enhanced vulnerability analysis tasks will also be conducted during the normative phase.

More details on how these security requirements are organized, collected and used to define a SAS for a specific Network Product Class are supplied in clause 5.2.2.4.

Once the SASs are ready, they will be used to define, when necessary, the expected test methodology for each security requirement in a dedicated document (for security compliance testing, basic vulnerability testing and enhanced vulnerability analysis tasks). This test methodology and skills requirements document is complementary to the expected output of the test cases defined in the SAS and should help the evaluators providing guidance on how to conduct these tests where necessary. This test methodology document will also define the expected skills and tools for testing laboratories (especially for Basic Vulnerability Testing and Enhanced Vulnerability Analysis).
Having an evaluation guidance document will help to ensure that the SECAM evaluations s can be compared to each other in the sense that a similar set of tools and techniques will be applied to produce the test outputs.
Besides, the "test methodology and skills requirements" document can be used by SECAM Accreditation Body as criteria to judge whether a tester has the necessary test skills required by the tests and then used to accredit the testers.

The SECAM Accreditation Body will define the administrative rules guiding the future evaluations (accreditation scheme for evaluators, dispute process).

NOTE 3: The detailed results of the testing from a network product are not expected to be public.
These results will be given to the operators upon request to the vendors and might also be requested by the SECAM Accreditation Body for resolution of dispute cases.

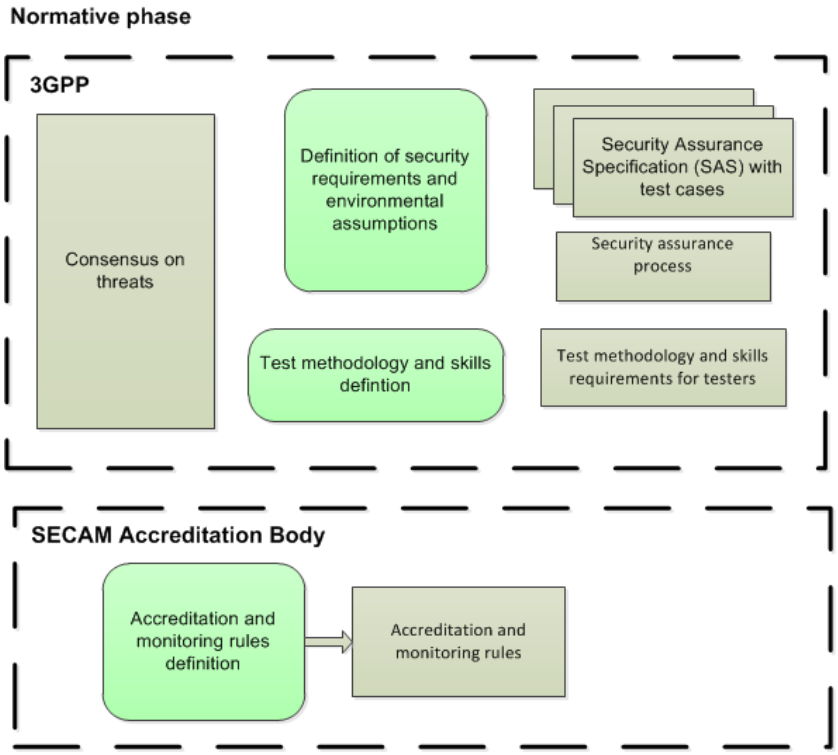


Figure 5.2.2.1-1: Successive activities for "Methodology 2" building

The writing of the security assurance process related document which will include Vendor Development Process Assurance requirements is detailed in clause 5.2.2.3. Clause 5.2.2.4 details the writing of the Security Assurance Specification documents which are used as input in the evaluation tasks.

The output of the security compliance task is detailed in clause 5.2.4.3. The output of the Basic Vulnerability Testing task is detailed in clause 5.2.4.4. The output of the Enhanced Vulnerability Analysis task is detailed in clause 5.2.4.5.

5.2.2.2 Security assurance process document creation

The security assurance process document will define the complete SECAM evaluation process (evaluation, relation to SECAM Accreditation Body, roles …) as well as the components of SECAM that are intended to provide the expected security assurance. It will thus describe for example 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. This 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 SASs for each network product class and not part of this overall process document. The same applies for vendor network product development and network product lifecycle management process requirements which will also be developed in a dedicated document (see clause 5.2.2.3).

In particular, during the normative phase, for each network product class there may be more than one document that applies to a given network product class. The documents contain different SAS modules as discussed in clause 4.1.3. Some SAS modules will serve as the reference document for security compliance testing while other SAS modules will serve as reference for the Basic Vulnerability Testing and Enhanced Vulnerability Analysis.

5.2.2.3 Vendor network product development and network product lifecycle management process document creation

Life cycle management consists in establishing discipline and control in the updates of network product during its development and maintenance. Life cycle 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 process will provide assurance for these aspects in SECAM.

Vendor network product development and network product lifecycle management process assurance requirements as well as related evaluation activities generic to all network product classes will be developed in a dedicated document. The requirements and evaluation activities for this task will be specified by SA3 in the normative phase; however Annex E of this document already provides an example set of requirements covering the four aspects below that could be included in the Vendor network product development and network product lifecycle management process assurance task:

- Version and Configuration Management;
- Flaw remediation;
- Process to ensure code quality;
- Vendors' development site protection.

The exact list of what categories have to be covered will be defined in the normative phase.

NOTE 1: Required and acceptable evidence needs to be defined in the normative phase to ensure comparability. Annex E describes concrete examples of requirements to cover these aspects with a list of required and acceptable evidences to ensure comparability

NOTE 2: Vendor network product development and network product lifecycle management process security quality is not a 3GPP/Telecom specific issue. The assumption is that for the normative phase, as much as possible from existing standards should be reused. During the normative phase four aspects could be covered (Version and Configuration Management, Flaw remediation, Process to ensure code quality and Vendor's development sites protection). Overall, similarly to the CPA Build Standard presented as example in Annex E, the number of requirements will have to be relatively small (an order of magnitude of 10) to keep evaluation cost reasonable and focus on critical controls.

5.2.2.4 Security Assurance Specification (SAS) creation

5.2.2.4.1 Writing process overview

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

- **Describe and model the network product class**
  I.e. the network product class shall be 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 selection of security requirements that are necessary and sufficient to solve the identified security problem.

- **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. CC part 2 [15] document will be used as a reference catalogue of security requirements and security requirement categories as a starting point to help SA3 in writing complete requirements.
  These requirements can and will be modified and adapted as seen necessary by SA3.
  SA3 will not be bound to the format of security requirements defined in CC part 2 (class, families, components…) and will be free for example to embed several dependencies of a security requirement directly in the requirement itself to ease readability and test case writing. Furthermore, 3GPP is not limited to modifying or adapting security requirements from CC part 2 [15] and may formulate their own security requirements when no suitable counterpart in [15] is found. When doing so care needs to be taken with respect to clarity, dependencies, and events to be logged, cf. also the following paragraphs. Further, when doing so, a rationale shall be provided explaining why it was necessary to deviate. It will be determined in the normative phase in which document rationales will be captured.

  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.

  Compliance with a CC protection profile format is not a goal as such, where it will be more efficient to deviate from it, SA3 will do so. The consistency of the requirements format is ensured by the template for a security requirement described in clause 5.2.2.4.2.3.3 hereafter.

  Security requirements in CC part 2 have dependencies between each other. For example, FMT_SMR.2 requires that there are restrictions on user-roles handling security functions. That is dependent on that also the security requirement FMT_SMR.1 is included. FMT_SMR.1 requires that there are roles defined for handling security sensitive assets (i.e., not everything is run as the root-user on *nix-like systems). These dependencies information will help SA3 to write sound requirements and should generally be included. There should be a rationale given for when modifications to the CC security requirements are required (e.g. removing a dependency). For each security requirement SA3 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 don't resolve any security objectives), the list of security requirements shall be updated accordingly by removing or adding security requirements.

5.2.2.4.2 SAS document structure and content

5.2.2.4.2.1 General

The SAS document contains three parts, a Network Product Class Description, a Security Problem Definition and the Security Requirements (including the test cases) for this specific Network Product Class [see clause 3.1], identified by SA3 to counteract the risks outlined by the threat analysis. Consequently each SAS document shall contain the following clauses:

- ***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.
- ***Security Problem Definition (SPD)***: This clause defines the security problem that is to be addressed and the security objectives of the network product class.
- ***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.

In the following a detailed description of each SAS clause is provided.

NOTE: References are made when analogous CC part 2 [15] requirements exist. The requirements in CC have names that follow this name format XYZ_VWU.n.mx. When the text below references the CC requirements that format is used, for example FMT_SMR.2.

5.2.2.4.2.2 Security Problem Definition (SPD)

For the Security Problem Definition clause of the SAS writing phase, the steps to be accomplished by 3GPP SA3 for a given network product class will be to:

- List the critical assets of the network product class;
- Identify the external interfaces of this 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 level of risk associated with the threats;
- 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 3GPP Technical Reports (e.g. TR 33.821 for EPS [20]) or other publications. In particular, threat analyses related to the security requirements in 3GPP TSs to be re-used in SECAM, cf. clause 5.2.2.4.2.3.2, need not be repeated in SECAM. These were however written before e.g. current SECAM type of work objectives came to light.

NOTE: 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.

There are also many threat and risks analysis or modelling frameworks available for IT equipment and computers networks. None of them is likely to perfectly fit the needs of SECAM which 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 the SA3 group gets the feeling 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.

Whatever the approach that will be chosen, the structure for this clause is provided 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 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

  - *Threat Description*: the adverse actions than 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, SA3 shall choose 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 shall then not be 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 4.5.2.2 and 4.5.2.3.

  - *Asset*: an indication of the network product assets object of the threat

  - *Risk:* a level of the risk related to the specific threat

  - *Security Objectives*: a concise and abstract statement that counter the identified threats. These security objectives shall be used to select the proper security requirements for the network product class under evaluation. The security objectives shall be on roughly the same abstraction level.

5.2.2.4.2.3 Security Requirements

5.2.2.4.2.3.1 Introduction

3GPP SA3 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 with associated test cases (as defined by the chosen methodology for SECAM)

- or operational environment assumptions that could also be documented in SAS for a given product class

The Security Requirements within the SAS document shall contain the security requirements identified according to the threats (see Figure 5.2.2.4.2.3.1-1).

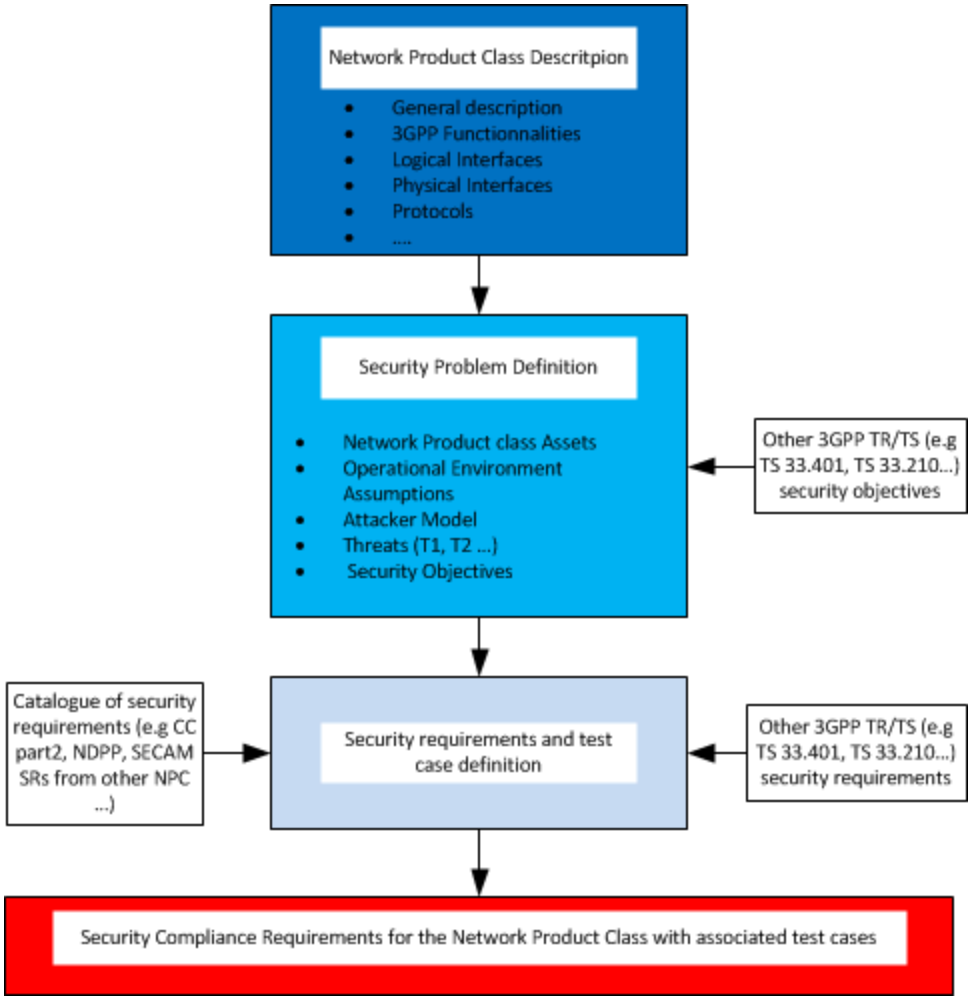


Figure 5.2.2.4.2.3.1-1: Process for deriving security compliance requirements in a SAS document

The security requirements will include security functional requirements as well as hardening 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 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, will be treated on the same footing and the text of clause 5.2.2.4.2.3 applies to both "types" of requirements. Their evaluation will be based on the tests cases of the SAS. In any case, hardening requirements test cases will imply that they must be implemented before evaluation. Hardening requirements should be formulated generic enough, or in different variants, to be applicable for a variety of anticipated OSs/applications/systems. Hardening is needed to let network products achieve the given security baseline and assurance level, alongside with other security functional requirements.

Hardening can be the removal of services, protocols, ports, etc, in order to reduce known security vulnerabilities and minimise 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 5.2.2.4.2.3.3.

SECAM security requirements represent the common agreement on 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 initialisation 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)

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

In Figure 5.2.2.4.2.3.1-1, 3GPP specifications represent an input for both SPD and Security Requirements and test case definition. The reason of this assumption is that 3GPP security specifications (e.g. TS 33.401 [8]) already contain several security objectives and relative security requirements which SA3 identified when designing UMTS and LTE. When looking at such type of security requirements, they can be grouped into three categories:

1) Security 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 requirement "The UE shall provide its equipment identifier IMEI or IMEISV to the network, if the network asks for it in an integrity-protected request" retrieved from TS 33.401, belongs to this category.

2) Security 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 requirement "The UE shall not send IMEI or IMEISV to the network on a network request before the NAS security has been activated" retrieved from TS 33.401 belongs to this category.

3) Security requirements not related to protocols and behaviours necessary for secure interoperability between nodes from different vendors, but rather deal with security features which shall be supported by the network products and consequently strictly related to their implementation.
For example, the requirement specified in clause 5.3 of TS 33.401 for eNBs and in annex I of TS 33.102 [21] for RNCs in exposed locations belong to this category.

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

The security requirements in the second category may not be covered by the interoperability and conformance testing. In this case a SAS document might contain a reference to these requirements with the relative test cases which verify that the network products are adhered to.

The security requirements in the third category are within the scope of SECAM and they will be taken into account in the Security Compliance Requirements. A security requirement retrieved from a 3GPP TS shall refer the relative TS requirement and shall also contain a test description to verify the correct implementation of the described security features (e.g. authentication and authorization for eNB settings and software configuration changes via local or remote access, key management requirements for the session keying material and long term keys used for authentication and security association setup purposes handled by eNBs, secure environment for eNB).

5.2.2.4.2.3.3 Handling of security requirements

A SECAM Catalogue of SRs is used as input for Security Requirements and test case definition task. The SECAM Catalogue of SRs has been introduce because it is likely that several network product classes will share very similar if not identical security requirements for some aspects. In order to maximize the reuse of already written requirements, it might be interesting in the normative phase to collect all security requirements written by SA3 into a single "catalogue" document. It would then be possible for the individual SASs of different network product classes to refer to it directly. This approach matches the requirement that a SAS 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 SAS (see clause 4.1.4 of the present document).

It is important to underline that the SA3 catalogue shall be constructed from existing SASs, and the intention is not to first create the catalogue and then write the first SAS based on it. No requirements shall be included in the catalogue before it has been included in a SAS. This prevents the catalogue from accumulating "good-to-have" requirements that are never used in real SASs. 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).

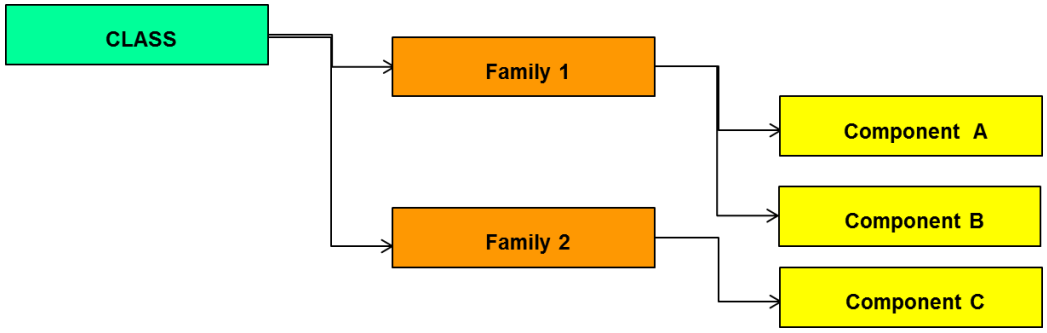
2) Select from the identified sources (for example, CC2, NDPP, OSPP) the proper security requirements that meet the needs of the security objectives and adapt them to SECAM.

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 (e.g. CC2, NDPP, OSPP) and update the Catalogue.

Usage of CC structure for requirements (class, family, components)

CC part 2 [15] group security requirements in class, family and components as shown in the picture below:



A class is a collection of security requirements assessing security risks or defined as a countermeasure to eliminate security vulnerabilities inherent to a given feature/capability. As an example the class "Security Management" covers the security risks the product administration introduces: sensitive information that normally is not transmitted across a network, such as product identifying information, configuration information, and other sensitive management information such as user names and passwords can be transmitted. The security requirements the network product shall be compliant to ensure that management does not expose this sensitive data to someone sniffing or eavesdropping on the network.

CC part 2 [15] contains the following classes:

- Security Audit: Security auditing involves recognising, recording, storing, and analysing information related to security relevant activities.

- Communication: This class provides two families specifically concerned with assuring the identity of a party participating in a data exchange (proof or origin, proof of receipt…).

- Cryptographic support: Cryptographic functionalities can be required to satisfy several high-level security objectives. These latter include (but are not limited to): identification and authentication, non-repudiation, trusted path, trusted channel and data separation. So this class provides mainly requirements on cryptographic operation and key management

    - -User data protection: This class provides requirements related to user data protection. - Identification and authentication: This class addresses address the requirements for functions to establish and verify a claimed user identity. Identification and Authentication are required to ensure that users are associated with the proper security attributes (e.g. identity, groups, roles, security or integrity levels).

- Security management: This class is intended to specify the management of several aspects of the TOE Security Functions: security attributes, data and functions. The different management roles and their interaction, such as capability, can be specified.

- Privacy: This class contains privacy requirements. These requirements provide a user protection against discovery and misuse of identity by other users.

- Protection of the TOE Security Functions: This class contains families of functional requirements related to the integrity of the mechanisms that constitute the TOE Security Functions and to the integrity of its own specific data.

- Resource utilisation: This class provides three families that support the availability of required resources such as processing capability and/or storage capacity.

- Resource Allocation provides limits on the use of available resources, therefore preventing users from monopolising the resources.

- TOE access: This class provides the functional requirements for controlling the establishment of a user's session

- Trusted path: This class defines the requirements to establish and maintain trusted communication to or from users and the TOE Security Functions.

During SAS writing SA3 may use these classes and grouping as guidance in order to ensure that no area of the network product class was missed.

As detailed in 4.1.4, SAS 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. The final choice of classes for this requirement catalogue is a normative phase activity. Whether SA3 choice will map the CC categories or not will depend on the number of requirements per classes and can only be decided when most of these requirements are already written.

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

Template for a Security Requirement Description

Editor's note: It is ffs whether an SAS should distinguish between mandatory and conditional requirements. If a function that is optional for a given network product class is present, then security requirements, made conditional on the presence of this function, will apply, otherwise not.

Statements of security requirements are intended to be clear, concise and unambiguous. A template for this purpose may follow the structure reported in this clause. In particular, each security requirement shall include:

- *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*: <capability class reference> - <the first two letter of requirement name>* or similar convention

    - *Requirement Description:* a detailed description for the security requirements identified by SA3 to reduce/counteract the risks outlined by the threat analysis.

    - *Threat reference:* the short identifier assigned to the threat, here used to mapping the requirement to the threat it intend to meet

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

    - *Requirement evidences:* the type of evidence that must be achieved, that is the expected test results

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 SAS 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 derivation of a security requirement from a CC part 2 requirement:

Even if the generic functional requirements are taken from CC Part 2, they have to be instantiated and refined, at least to the extent that they are meaningful to fulfil and still remain applicable to all network products of the network product class.

Dependent requirements are not required to be included and can be skipped if a short rationale is provided for why it is acceptable to do so. It will be determined in the normative phase in which document rationales will be captured.

An example of audit generation FAU_GEN.1.1 taken from the OSPP v3.9 and NDPP v1.1:

This is the requirement as specified in CC3.1R4 Part 2	FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events: a) Start-up and shutdown of the audit functions; b) All auditable events for the [selection, choose one of: *minimum, basic, detailed, not specified*] level of audit; and c) [assignment: *other specifically defined auditable events*].
This is how it is instantiated in OSPP v3.9	FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events: a) Start-up and shutdown of the audit functions; b) All auditable events for the **not specified** level of audit; and **c) all modifications to the set of events being audited;** **d) all user authentication attempts;** **e) all denied accesses to objects for which the access control policy defined in the OSPP base applies;** **f) explicit modifications of access rights to objects covered by the access control policies; and** g) **other specifically defined auditable events as defined in the table in FAU_GEN.1.2.**
This is how it is instantiated in NDPP v1.1. **Note that the dependent requirement FPT_STM.1 is include and that the additional requirement FIA_UIA_EXT.1 shows additional events that shall be logged.**	FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events: a) Start-up of the audit functions; b) All auditable events for the **not specified** level of audit; and c) **All administrative actions;** d) **Specifically defined auditable events listed in Table 1**. **Table 1 – Auditable events and audit record content:** **FIA_UIA_EXT.1** **All use of the identification and authentication mechanism. (Provide user identity, origin of the attempt, e.g., IP address).** **FPT_STM.1** **Changes to the time. (The old and new values for the time. Origin of the attempt, e.g., IP address).** […]

The SAS may add explicit tests to these requirements. For example, the test whether "Start-up and shutdown of the audit functions;" is performed by the network product, the product can be started and then stopped and the log can be examined if these events get properly logged.

Here is a concrete example of an instantiation of FAU_GEN.1.1 in the Template for a Security Requirement Description:

- *Requirement name:* Security audit data generation
  - *Requirement reference:* FAU_GEN.1.1 (or something else if it becomes necessary to use a different nomenclature to point out that there may be differences compared to CC).
  - *Requirement Description:* The TSF shall be able to generate an audit record of the following auditable events:
    - Start-up of the audit functions;
    - All auditable events for the not specified level of audit; and
    - All administrative actions;
    - Specifically defined auditable events listed in Table 1.
    - Table 1 – Auditable events and audit record content:
      - FIA_UIA_EXT.1 All use of the identification and authentication mechanism. (Provided user identity, origin of the attempt, e.g., IP address).
      - FPT_STM.1 Changes to the time. (The old and new values for the time. Origin of the attempt, e.g., IP address).
      - […]
  - *Threat reference:* T1, T2, T3
  - *Test case:* Start node and examine if log contains start up event. Login as administrator and examine if log contains the login attempt. Expected tools include log-reader. The skills required by the tester are ability to generate the events and using the log-reader. ...

- *Requirement evidences:* A document in free form describing which events were generated, the output from the log-reader.

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.
  - *Threat reference:* T1, T2, T3;
  - *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
  - *Requirements evidences:* A document in free form describing: the services listening on each physically accessible port and the type of credential required for access and the output from the different scanning tools.

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

5.2.2.5 Security Assurance Specification instantiation documents creation

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

The SAS instantiation is a set of documents and is not expected to have a fixed structure. This will allow Vendors to maximise the reuse of existing documentation.

The content of the SAS instantiation is however defined and it shall contain details on:

- Network Product description (e.g. software version, documentation version)
- Scope of evaluation
- Mapping of SAS 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, Basic Vulnerability Testing and Enhanced Vulnerability Analysis

This document set is updated by the Vendors until the testers (Security Compliance Testing, Basic Vulnerability Testing and Enhanced Vulnerability Analysis) 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 5.2.4.2.

5.2.2.6 Accreditation and monitoring rules creation

SECAM Accreditation Body shall describe the rules for accreditation and monitoring of development and test laboratories, whether they are vendors or third-party laboratories. A formalised dispute resolution process for accreditation and monitoring is likely to be required as the denial or delay of accreditation may have far-reaching consequences.

5.2.3 Vendors and third-party laboratories accreditation

5.2.3.1 Overview

NOTE: The final choices and rules for the accreditation and monitoring rules are under the responsibility of the SECAM Accreditation Body. This clause still describes this process for the sake of completeness by giving examples of possible rules.

In order to be allowed to conduct the evaluation, the vendors or third-party laboratories must demonstrate they have the skills, working practices and resources to participate in the process.

This can be achieved e.g. by a combination:

- an evaluation of general methodology skills (through an ISO 17025 accreditation – applicable to vendors test laboratories or third-party test laboratories only) (see 5.2.3.1)
- an "audit and accreditation" by the SECAM Accreditation Body to demonstrate that the Evaluators have the necessary skills. It would be up to the SECAM Accreditation Body to indicate how the evaluator can demonstrate their competency in conducting an evaluation for conformance to 3GPP SAS requirements. (see 5.2.3.4)

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

- a quality qualification (see 5.2.3.2)
- an audit and accreditation of network product development and network product lifecycle management process (see 5.2.3.3)

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

Figure 4 hereafter shows the main phases of an accreditation processes.

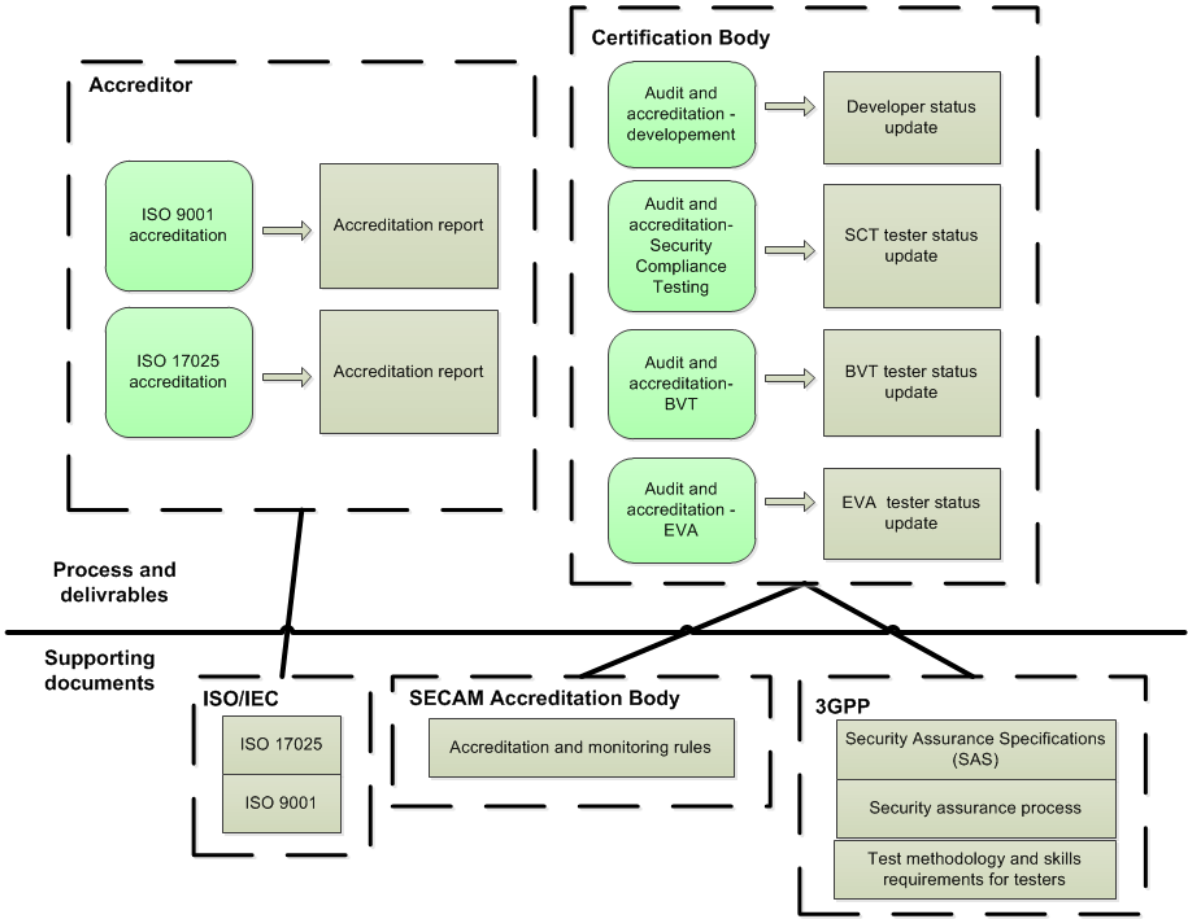


Figure 5.2.3-1: Accreditation of vendors or third-party laboratories by SECAM Accreditation Body

5.2.3.2 Methodology and quality accreditation

SECAM resorts to already established and widely recognized accreditation bodies to assess the methodological practice of testing laboratories, whether they perform Security Compliance Testing, Basic Vulnerability Testing or Enhanced Vulnerability Analysis. It also relies on these bodies for the Quality Qualification for Vendors. These generic methodological practices (quality system of the testing laboratories, ability to calibrate tools …) and quality qualification for vendors are not SECAM specific and thus for these tasks, the SECAM Accreditation Body will rely on already well-recognised national accreditation bodies in this area.

Ideally, accreditation bodies involved in SECAM-related accreditation are directly worldwide operating and recognized organizations or national bodies participating in an internationally recognized umbrella organization covered by a Mutual Recognition Arrangement (MRA).

E.g. the ILAC (International Laboratory Accreditation Cooperation, https://www.ilac.org/) full members are signers of the ILAC MRA which amongst others includes the mutual recognition of ISO 17025 (General requirements for the competence of testing and calibration laboratories) accreditations.

Example of national accreditation bodies being signers of the ILAC MRA are:

- ANSI-ASQ / ANAB in the USA;
- CNAS in the People's Republic of China;- ACCREDIA in Italy;
- COFRAC in France;
- DAkkS in Germany;
- UKAS in the United Kingdom;
- JAB in Japan;

- KOLAS in the Republic of Korea;
- etc. (about 80 ILAC MRA signers in total)

For SECAM specific aspects (clause 5.2.3.3 and clause 5.2.3.4), the responsible body for accreditation is the SECAM Accreditation Body.

Quality qualification for Vendors

To ensure that the manufacturer's design, development and manufacturing processes are, and remain, compliant with a recognised quality assurance standard, the manufacturer's quality system must be under regular review as part of an accredited activity via for example an ISO 9000 or an appropriate regional equivalent accreditation.

Methodology Accreditation for vendors or third-party testing laboratories

To ensure that the methodological practice of vendors or third-party testing laboratories are, and remain, compliant with a recognised standard, the vendors or third-party testing laboratories must be under regular review as part of an accredited activity via for example an ISO 17025 or an appropriate regional equivalent accreditation.

5.2.3.3 Audit and accreditation of Vendor network product development and network product lifecycle management process

The evaluation of the security relevant part of the Vendor network product development and network product lifecycle management process is done as part of the vendor accreditation process by the SECAM Accreditation Body.
The network product development process and network product lifecycle management process document detailing the accreditation requirements and test cases is the one described in clause 5.2.2.3.

The Vendor network product development and network product lifecycle management process assessment covers a Vendor's engineering processes and does not necessarily apply only to a single network product. That means that the results of one assessment may apply to more than one network product. The Accreditor mandated by the SECAM Accreditation Body should note in the accreditation where there is evidence to suggest that the scope of the validation is unlikely to apply to more than one network product.

Vendors can get their generic network product development and network product lifecycle management process or a subset of it accredited. A generic network product development and network product lifecycle management process is 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 gets accredited 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 process compliance validation" task (cf. 5.2.4.1) 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 (see 5.2.4.2 for details).

NOTE 1: The requirements on the process and acceptable evidences ("test cases") will be defined by SA3. However the definition of way to get an accreditation for these requirements is under the responsibility of the SECAM Accreditation Body which will have to deal with the cost/complexity/assurance trade-off. It should be avoided that vendors need to obtain a large number of accreditations for their network product development and network product lifecycle management process.

NOTE 2: The Vendor is expected employ Industry related good working practices, aligned to the relevant parts of the ISO/IEC 27000 series. Although these areas will not be formally audited by the Accreditor mandated 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. Moreover, the test cases for the SECAM requirements are expected to leave room to the vendor to reuse evidences from these previous accreditations and thus reduce costs.

5.2.3.4 Audit and accreditation of testing laboratories

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

- assessing the skills of the vendors or third-party laboratories in conducting an evaluation for conformance to 3GPP SAS requirements for a given network product class or range of classes;

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

One can be accredited for Security Compliance Testing, Basic Vulnerability Testing or Enhanced Vulnerability Analysis or for all four of them. The audit for the accreditation is typically performed during an evaluation session where the testing laboratory demonstrates its skills to an auditor from the SECAM Accreditation Body by undertaking the tests on a concrete network product.

NOTE: An accreditation might only be applicable to a given LTE network product class, since it assesses the technical skills of the testing laboratories. The requirements on the network product classes and acceptable evidences ("test cases") will be defined by SA3. However the definition of way to get an accreditation for testing these requirements and the definition of the coverage of the accreditation (for one or for several network product classes, and/or for testing) is under the responsibility of the SECAM Accreditation Body which will have to deal with the cost/complexity/assurance trade-off. It should be avoided that laboratories, vendor or a third party need to obtain a large number of accreditations

5.2.3.5 Criteria on accreditation of security compliance testers laboratories

NOTE: It is FFS at the time the accreditation criteria are actually defined what suitable means to assess individual skills are. All suggestions for such assessments stated here are ideas how that could be done. In general, when it is not guaranteed that assessments are done in a manner that are efficient in serving their purpose and are deterministic in their outcome they don't need to be executed in the first place. Therefore it needs to be studied in detail how efficient they are and it must be ensured that they are reproducible before they are used.

The accreditation is expected to determine that the security compliance testing laboratories have:

- Sufficient auditing skills to assess that the Vendor provided enough evidences that the network product is following the "Vendor development and lifecycle management" accredited process

- Accurately describe their test procedures, results and conclusions

  - such skills might be assessable through a case study or a "pilot" evaluation performed under the supervision of the accreditor.

- Capacity to assess the consistency between a SAS and an instantiated SAS

- Capacity to assess the coverage of the SAS / instantiated SAS by tests

  - Such skills might be assessable by an examination showing the knowledge of the SAS, and a case study to assess the rigour when determining the coverage of SAS by a given instantiated SAS

- Define a representative testbed for a given network product:

- Perform representative and complete tests derived from the SAS:

  - Such skills might be assessable by an oral examination showing the general knowledge of the considered network product, in particular

    - Protocols and interfaces

    - Administration and deployment issues

  - The skills necessary to perform the Security Compliance Testing required by the SAS will depend on the nature of the SAS tests defined in the normative phase (e.g. "black-box" testing, code auditing, documentation review …)

    - Such skills might be assessable by a case study examination conducted by the accreditor

- Accreditation could consequently be performed separately for different network products, and a tester could be accredited only for some products

- a "pilot" evaluation performed under the supervision of the accreditor could also be considered as a mean to assess those skills as a whole.

5.2.3.6 Criteria on accreditation of Basic Vulnerability testers laboratories

Editor's note: It is FFS whether the skill set for this activity is different from the one from the compliance testers' laboratories or whether it is similar. Whether this separate activity could be run by the compliance testers' laboratories to keep the methodology simple and limit the number of actors and accreditation is also FFS.

5.2.3.6 Criteria on accreditation of Enhanced Vulnerability Analysis (EVA) testers laboratories

The Accreditation Body shall administer the assessment of relevant criteria, standardized in the normative phase, to determine that the EVA testers have sufficient skills and administer the assessment. The following are possible assessment scopes and techniques:

- Accurately describe their test procedures, results and conclusions.

  - such skills could be assessed through a case study or a "pilot" evaluation performed under the supervision of the accreditor.

- Capacity to assess the security consistency between the SAS and an instantiated SAS, especially the capacity to assess whether the attacker model stays consistent within the environment described in the instantiated SAS:

- Capacity to determine if certain attacks are within the scope of the attacker model:

- Sufficient skills to perform an impact analysis of a vendor update of the network product;

  - Skills also include general penetration testing methodology capacities; such skills could be assessed by a case study examination conducted by the accreditor

- Capacity to assess the consistency of TOE/TSF in a given network product, especially capacity to assess that environmental assumptions are not used to waive security functionalities required by the SAS:

- define and perform representative and complete tests:

  - Such skills could be assessed by an oral examination showing the general knowledge of penetration testing in the considered network product

  - Accreditation could consequently be perform separately for different network products, and an tester could be accredited only for some products (e.g. only for core network products)

  - a "pilot" evaluation performed under the supervision of the accreditor could also be considered as a mean to assess those skills as a whole.

5.2.4 Evaluation and evaluation report

5.2.4.1 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 initial accreditation administrated by the SECAM Accreditation Body according to 5.2.3.3 prior to any network product evaluation. During a network product evaluation, the compliance testing laboratories validate that effectively the accredited process was used for the network product under consideration. To allow this evaluation, the vendor shall provide the following documents to the compliance testing laboratories and, if requested, to the operator:

- The Vendor network product development and network product lifecycle management process accreditation certificate from 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]

The compliance testing laboratories will review this self-evaluation report and evaluate if the rationale provided by the Vendor provides enough evidences that the network product is following the accredited process.

If the report is acceptable, the evaluation continues. If not, the testing laboratories request the vendor to get accredited for the process of this network product as well. In most cases, compliance testing will be undertaken by the vendors themselves and conflict are expected to be rare. However, the compliance testing laboratories take a responsibility in this assessment as the rationale and the description of the generic accredited process will also be given to the operators which are likely to review them as well. Conflict between vendors, testing laboratories and operators will be resolved by the SECAM Accreditation Body.

NOTE: Required and acceptable evidence for the vendor Network Product Development and network product lifecycle management process self-evaluation report need to be defined by the SECAM Accreditation Body to ensure comparability and easy conflict resolution if any.

5.2.4.2 SAS instantiation evaluation

5.2.4.2.1 Overview

SAS instantiation evaluation is to check whether an SAS instantiation written by a vendor is a correct instantiation of the SAS 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 SAS instantiation evaluation before it is used to evaluate network product. The evaluator shall confirm at least that the SAS being instantiated for a given 3GPP network product and the network product for evaluation are consistent,

5.2.4.2.2 Content

5.2.4.2.2.1 Scope of evaluation

5.2.4.2.2.1.1 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. For example, vendor A might package and commercialized its MME network product Z1 as an application only with the operator being responsible to provide the hardware and the virtualisation environment to run this MME network product. In some individual cases, some operators might however request that the vendor provides a complete bundle (including hardware and virtualisation solution) in addition to the MME application Z1.

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. These definitions are provided in the scope of evaluation description provided by the vendor in the SAS instantiation by a definition of the TOE and TSF as developed in 5.2.4.2.1 and 5.2.4.2.2.

CC uses different terms to define what is to be evaluated, namely Target of Evaluation (TOE) and TOE Security Functionality (TSF). Given the differences between Common Criteria and Methodology 2 approaches, those terms are not necessarily identical to their CC counterparts. Clarifications on the differences are provided in the dedicated clauses.

NOTE: SECAM provides no provision to assess whether the evaluation results for a different package of the network product that 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 SAS instantiation, the operator can make their security acceptance decision with a clear understanding of what was evaluated for this new package.

Editor's note: The intention of the text of clause 5.2.4.2.2 and clause 5.2.4.2.3 to have clear TOE and TSF definitions is agreed. The intention of these clauses is to ensure that the flexibility introduced for the TOE cannot be misused to limit the part of the network product subjected to the evaluation against the SAS. The wording of these clauses however has to be improved to make a clearer distinction between what is related to requirements on TOE content and what is related to requirements on TOE description

5.2.4.2.2.1.2 TOE

Editor note: In SECAM, the generic network product class definition will be defined in the SAS. The vendors will instantiate these definitions in their SAS instantiation by describing the TOE and the TSF of their Network Product based on the requirements below. How to properly name the generic network product class description in the SAS to avoid confusion with the TOE TSF definition for evaluation below is FFS.

The TOE defines what, within the commercialized Network Product, is to be evaluated. It is defined Common Criteria as "a set of software, firmware and/or hardware possibly accompanied by guidance." In CC, the TOE is defined by the vendor. In CC evaluations not following a Protection Profile there is a huge latitude for the vendors in this definition, since a vendor may choose to include components in, or exclude them from, the TSF at free will. This latitude does not exist for SECAM since the TSF for the entire network product as commercialized by the vendor is defined by the available and applicable SASs.

In order to ensure that the TOE is sufficiently comprehensive and well described, the definition here shall comply with the following requirements:

- All requirements from the SAS(s) pertaining to the network product class shall be reflected in the TOE. All interfaces of the TSF shall be part of the description of the TOE. This defines a condition for a minimum size of the TOE.

Editor's note: If SA3 decides to make a distinction between mandatory and conditional requirements (see clause 5.2) the formulation in the above bullet will have to be adapted to 'all APPLICABLE requirements' or similar

- All external communication interfaces of the TOE shall be part of the TOE description. External communication interfaces of the TOE are interfaces that allow communications between functions inside and outside the TOE. If the TOE is not the entire product as packaged for evaluation then the interfaces between the TOE and the parts of the network product not in the TOE need to be described as external communication interfaces of the TOE. Justification why it is not possible to access the assets of the network product as defined per the SAS by other means that the external interfaces of the TOE must be provided.

NOTE 1: The Basic Vulnerability Testing will be conducted on the external communication interfaces of the TOE. If the TOE definition is smaller than the entire network product, the above requirement makes possible to have external communication interfaces of TOE under evaluation that are not in the set of external communication interfaces of the network product. Testing these external interfaces of the TOE which might be potentially internal interfaces of the network product might be challenging. Moreover, proving that the above mentioned justification is valid might be challenging. Thus reducing the scope of the TOE to a smaller subset than the network product does not guarantee easier testing.

NOTE 2: this requirement is to ensure that these interfaces are covered by the BVT and EVA. It also ensures that no external interface to the product not covered by the TOE can be used to attack the TOE as such attacks would have to go through an external communication interface of the TOE.

- A TOE is allowed to be larger than this minimum size defined by the preceding bullets. NOTE1 above explains why this may be useful.

5.2.4.2.2.1.3 TSF

CC also defines TSF as the "combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the Security Functional Requirements". In CC, the vendor has latitude

regarding the definition of TSF interfaces in terms of *granularity* (entire process supporting the security function, API within this process, physical interface of the board embedding the process…).

In SECAM, the context is different, because the tests are already described, although at a high level, within the SAS. In SECAM, the TSF would be a "combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SAS requirements". Whether a component is part or not of the TSF as well as the granularity of the definition of a component is disambiguated by the test cases of the SAS. For example an SAS 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 SH server is listening).

The SAS instantiation shall not exclude a component from testing on the grounds that it was already evaluated under another scheme unless this SAS allows it explicitly to refer to the certificate obtained under this different scheme for a given set of tests (e.g. FIPS).

Editor's note: Whether SECAM recognizes the results of other evaluation (for example FIPS) and requires re-testing is FFS

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

5.2.4.2.2.2 Mapping of SAS security requirements to the network product and assets in the network product

The SAS instantiation will provide:

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

The evaluator shall confirm at least that:

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

NOTE 1: e.g. the SAS instantiation shall not decide, against the SAS, that some assets need no protection because of physical deployment site protection

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

NOTE 2: e.g. if the SAS instantiation uses two admin roles instead of a single one in the generic SAS, both shall have their credentials protected consistently

- the SAS instantiation does not waive threats identified in the SAS,

NOTE 3: e.g. the SAS instantiation shall not claim that a threat from the SAS is not applicable under the assumption that more organizational control is performed during administrators' recruitment

5.2.4.2.2.3 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 SAS instantiation documentation (see 5.2.4.2 for details on SAS instantiation evaluation). This documentation contains the

information on how to initialize, configure and operate the network product so that SECAM security requirements are met. The network product and the content of the "operational guidance documents" must be fully aligned.

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 MUST 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 must be followed in full.

NOTE 1: As part of SAS 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.

5.2.4.2.2.4 Information needed to execute the required tests for SCT, BVT and EVA activities

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

The compliance tester shall assess whether the SAS instantiation contains enough information to:

- install a representative testbed;

Editor's note: The definition of "representative" is FFS.

- define test vectors;
- perform tests;
- determine whether the tests completely and accurately cover the SAS.

Editor's note: The relation between the "Test Methodology and skill requirements "document and the bullet above has to be clarified.

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

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

Information needed to execute the required tests Enhanced Vulnerability Analysis:

The EVA tester could be required to assess whether the SAS instantiation contains enough information to:

- define relevant attack paths;
- perform penetration tests following these attack paths;

- determine whether a found possible Vulnerability is exploitable in practice, within the operational environment of the product;
- determine whether their tests cover what would be expected from the type of attackers defined in the SAS attacker model;
- eventually conclude whether the network product resists the type of attacks that are expected from the attacker model defined in the SAS.

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

5.2.4.2.3 Process

The usage and update of this set of document during a SECAM evaluation is described in Figure 5.2.4.2.3 below.

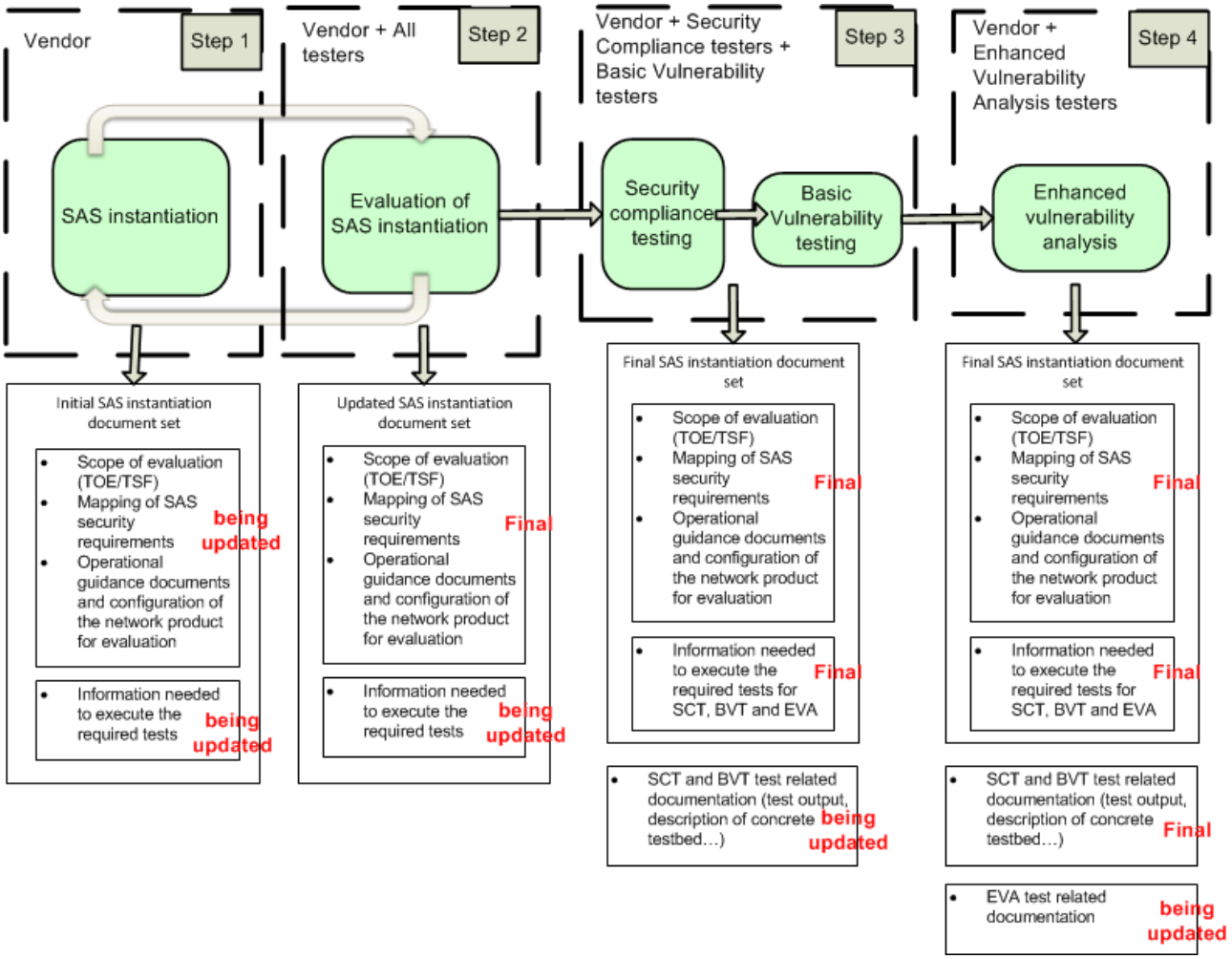


Figure 5.2.4.2.3-1: Overview of the SAS instantiation documents evolution during a SECAM evaluation

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 SAS instantiation evaluation to check whether an SAS instantiation written by a vendor is a correct instantiation of the SAS of the network product class and whether it is a good basis for evaluating the network product. All accredited testers (SCT, BVT and EVA) are required to assess the SAS instantiation before it is used to evaluate network product. This assessment has two main goals

- Assessing that the vendor documentation and processes are complete sufficiently defined to begin the evaluation
- Validating the elements (scope of evaluation, instantiated assets…) which must not be modified during the evaluation

For example, should the scope of evaluation be modified between SCT, BVT and EVA testing, the whole compliance evidences would be obsolete (since the interfaces, in particular, may have changed). For this reason, all testers are expected to synchronize from the beginning of evaluation in order to agree on a scope.

NOTE: During the normative phase, it shall be decided which information can or cannot be modified without a new assessment and approval from all, SCT, BVT and EVA testers. The goal is to have an early validation from SAS instantiation from all testers to avoid that compliance tests or basic vulnerability testing are nullified and must be redone before the Enhanced Vulnerability Analysis.

Step 3 and 4 are the regular SCT+BVT and EVA testing tasks of Methodology 2 which will use this instantiation documentation as input. The evaluation shall not start (neither SCT nor BVT nor EVA) as long as steps 1 and 2 are not completed. It is of outmost importance that all the aspects below are agreed by both evaluators in step 2 before the evaluation start to ensure consistency in the results of step 3 and step 4.

Further documentation is produced during step 3 and 4. During step 3 for example, the Security Compliance tester 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 SAS test case). At the end of step 4, the SAS instantiation documentation as well as the SCT, BVT and EVA documentation is an output document provided to the operator. These documents are described in 5.2.4.3 and 5.2.4.4.

After step 4, all the output documents of step are given to the operator for its final review and final security acceptance decision.

5.2.4.3 Security Compliance testing

5.2.4.3.1 Inputs

The test bed configured according to the documentation that was produced in step 2 of clause 5.2.4.2.2.

5.2.4.3.2 Outputs

In the end of Security Compliance tests, the tester will deliver:

- 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, the Security Compliance tester should 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 shall be
  - 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 SAS test cases

- the test procedure followed in practice [following SAS test cases] and results [following SAS output format indications];

5.2.4.3.3 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 security assurance specification following the template of 5.2.2.4.2.3.3. Many examples of requirements are available in Annex A.2. The test case describes the validation technique to be used by the Security Compliance Testing laboratories as well as the expected outputs to provide in the evaluation report. It is worth noting that, at least a test case is defined for every security requirement, since every security requirement should lead to

- *positive* tests (the network product performs as expected when operated correctly with correct inputs)

- *negative* tests (the network product correctly handles error cases such as incorrect usage or incorrect inputs)

3GPP SAS specifications provide guidelines for the type of tools to be used for the validation of these tests. This test case describes the validation technique to be used by the security compliance testing laboratories as well as the expected outputs to provide in the evaluation report.

Security compliance testing laboratories execute the tests contained in the 3GPP SAS for the evaluated network product as described in the test cases, collect evaluation evidences and include them in the final security compliance report (see clause 5.2.4.3.2 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.

5.2.4.4 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 expected to be specified as a general SAS module. This general SAS module will then be linked and potentially amended by SASs 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. The protocols for which the individual Basic Vulnerability Testing activities will be required are to be selected during the normative phase.

NOTE 3: The individual tools used for Basic Vulnerability Testing are selected by the Security Compliance Testing 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. Details can be found in Annex A.2.1. The Basic Vulnerability Testing laboratories shall provide to the operator:

- the test procedures [following SAS (see Annex A.2.1)]

- the test results [following SAS output format indications (see Annex A.2.1)]

5.2.4.5 Enhanced Vulnerability Analysis task

NOTE 1: Threat assessment data and description of key assets of network products provided by the vendors will help the evaluator in understanding the product under evaluation. It is FFS which documents are needed to fulfil this need. This will be subject of a dedicated future Study Item on EVA.

NOTE 2: Enhanced Vulnerability Analysis will be done based on SAS scope

NOTE 3: As for how to do the Enhanced Vulnerability Analysis the SAS document may provide a test description and an indication of the tools and test methods to be used (see 5.3.4.4.3 Activities).

NOTE 4: In the current version of the TR it is not clear in which document and by whom the set of tools and methods to be used for this task will be defined. This must be clarified. This will be subject of a dedicated future Study Item on EVA.

5.3.4.4.1 Inputs

The test bed configured according to the documentation produced in step 2 (see 5.2.4.2.2)

5.3.4.4.2 Outputs

Enhanced Vulnerability Analysis laboratories execute the tests for the evaluated network product, collect evaluation evidences and include them in the final security vulnerability test report, which will include at least (following a document "Test Methodology and skills requirements" :

- Declaration about who carried out the tests (e.g. self-evaluation or third party Evaluators).
- the test procedure, including
  - the attack paths and vectors used for the tests;
  - Vulnerability library to which this test refers to
  - The reference model/method/testing tool used for Enhanced vulnerability analysis.
  - Network products/features tested and reasons for not testing where applicable.
- The test results [following SAS output format indications] containing
  - Vulnerabilities that were to be tested and correctly addressed by the product,
  - Residual vulnerabilities not addressed by the product;
    - A list of these residual vulnerabilities prioritized by their e.g. CVSS score, with the associated risks to which the operator can be exposed to. The impact assessment about exploitable vulnerabilities in the network product are based on the deployment assumptions listed in the SAS, e.g. the possibility that vulnerability can be used for attacking, e.g. remote attacking, how serious damage can be made through this vulnerability, etc.

Editor note: It is FFS which ones of these elements should be archived in tester premises (for confidentiality reasons); included in the evaluation report; included in the instantiated SAS.

NOTE: The EVA report should not be issued to the public, it can only be kept between the party generating the report and the party receiving the report.

5.3.4.4.3 Activities

EVA of a network product could e.g. consist in exploiting vulnerabilities for a given attacker model for EVA.
An attacker model for EVA consists in a scale of attacker type and levels; levels could be determined by a list of criteria such as expertise or time available for the attack. This attacker model for EVA could be defined in the SAS.
This definition could be used for two different activities:

- the accreditation of testing laboratories (verification by the SECAM Accreditation Body that the testing laboratories have the skills)
- during the evaluation itself. The accredited tester only performs attacks (time, material…) that are in line with the model defined in the SAS

Testers could use:

- Publicly available information on vulnerabilities coming from a range of known vulnerabilities documented in some vulnerability library, e.g. CVE (Common Vulnerabilities and Exposures, "a publicly available and free to use list or dictionary of standardized identifiers for common computer vulnerabilities and exposures" by the MITRE Corporation, an US not-for-profit organization. http://cve.mitre.org/), CWE (Common Weakness Enumeration, "a community-developed dictionary of software weakness types" also by the MITRE Corporation. http://cwe.mitre.org/) , and other FIRST (Forum for Incident Response and Security Teams, "brings together computer security incident response teams from government, commercial, and educational organizations", http://www.first.org/), TCG (Trusted Computing Group, "a not-for-profit organization formed to develop, define and promote open, vendor-neutral, global industry standards, supportive of a hardware-based root of trust, for interoperable trusted computing platforms.", www.trustedcomputinggroup.org) identified vulnerabilities etc.

- Attack paths definition

- More advanced tools than those used for Basic Vulnerability Testing

Editor's note: Clarification on what "Attack path" means, in which document this will be defined and by which entity (SA3 or SECAM Accreditation Body) is needed. This will be subject of a dedicated future Study Item on EVA.

5.2.5 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.

Editor's note: Further details can be provided after the study phase.

NOTE: Ideally both vendors and operators would prefer everything (all tests, requirements, processes etc.) are passed or met, but in reality there may be vulnerabilities in a product or security functions that are not fully developed. A self-declaration doesn't mean all security requirements are met or no vulnerabilities can be found in the product. The self-declaration can also imply partial compliance. The vendors need to summarize the evaluation results truthfully in self-declaration. It is up to the operators to make the final decision whether the product can be accepted or not.

5.2.6 Operator security acceptance decision

The operator examines the network product, the security compliance testing, basic vulnerability testing and Enhanced vulnerability analysis reports, the self-declaration as well as the testing laboratories certificate published by the . SECAM Accreditation Body 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, basic vulnerability testing or enhanced vulnerability analysis, 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.

5.2.7 Administration of the accreditations and dispute resolution

5.2.7.1 Monitoring

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

- Vendors development processes, which are expected to comply with the Security Assurance Process

- Security compliance testing laboratories, which are expected to comply with the Test Methodology and skills requirements

- Basic Vulnerability Testing laboratories, which are expected to comply with the Test Methodology and skills requirements
- Enhanced Vulnerability Analysis laboratories, 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)

5.2.7.2 Dispute resolution

The SECAM Accreditation Body must provide 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);
- Security compliance testing laboratories activities (inconsistencies in analysis of compliance against SAS);
- Basic Vulnerability Testing laboratories activities (inconsistencies in analysis or use of the output of the BVT tools);
- Enhanced Vulnerability Analysis laboratories activities (inconsistencies in analysis of residual vulnerabilities).

The SECAM Accreditation Body typically performs a supplementary audit on vendor / third-party laboratories premises and updates their accreditation records.

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 conflict resolution and revocation 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. GSMA might be a good candidate as they are already involved in GCF and GSMA SAS scheme (http://www.gsma.com/technicalprojects/fraud-security/security-accreditation-scheme).

At the end of the dispute procedure, if the entity responsible for it decides so, the accreditation of the different actors would be revoked and added to the accreditation revocation list. Consequently, results of network products evaluations for evaluations conducted by these revoked actors would be considered untrusted.

5.2.8 Summary of SECAM deliverables

Phase	Sub-phase	Deliverable	Published by
Methodology building		Consensus on threats [temporary document]	3GPP
		Security Assurance process	
		Network product development and network product lifecycle management Process Assurance requirements	
		Security Assurance Specifications for the network product class listed in clause 4.4	
		Test methodology and skills requirements	
		Testing laboratories accreditation and monitoring rules	SECAM Accreditation Body / GSMA
Accreditation	Methodology Accreditation	Accreditation report	Accreditor
	Audit and accreditation	Vendor network product development and network product lifecycle management process certificate Security Compliance testing laboratories certificate Basic Vulnerability Testing laboratories certificate Enhanced Vulnerability testing laboratories certificate	SECAM Accreditation Body / GSMA
Evaluation	SAS instantiation	Instantiation of SAS	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	Test procedures [following SAS] Test results [following SAS output format indications]	Vendor or third-party
	Basic Vulnerability Testing	Test procedures [following SAS] Test results [following SAS output format indications]	
	Enhanced Vulnerability Analysis	Test procedures [following Test methodology] Test results [following SAS output format indications]	
Self-declaration	Self-declaration	Self-declaration	vendor
Monitoring, dispute resolution		Informal guidance document. Accreditation revocation list	SECAM Accreditation Body / GSMA
Dispute resolution	-	Operator claims	

5.2.9 General considerations

5.2.9.1 Improvement of SAS and new security requirements

Vendors, operators or other bodies can propose new security requirements for addition to 3GPP standards (SAS) if a new threat or vulnerability has been identified. This gives SA3 the flexibility to continuously review and improve their security compliance checklist.

5.2.9.2 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 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 will describe 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 evaluation report results. The final security acceptance decision is under

operators' control which might accept partially compliant products. This choice under operators' responsibility and is outside of SECAM scope.

5.2.9.3 Comparison between two SECAM evaluations

SECAM evaluation considers a given version of a network product. SECAM documents will have no sections or evaluation of the improvement between two evaluations.

6 Criteria for the evaluation of the methodologies

Editor's Note: This clause will list the criteria that will be used to evaluate the proposed solution (type of attacks conducted, reproducibility of the tests, costs, international recognition, need for coordination with other bodies ...)

Editor's note: Part of the methodologies relates to producing SAS another part of the methodologies relates to evaluating how product are fulfilling requirements of these SAS. Criteria's addressing both aspects have to be defined.

The 3GPP security assurance methodology under consideration should be evaluated based on the following evaluation criteria:

NOTE: Effort required for security assurance should be commensurate with confidence gain. Therefore candidate methodologies may not necessarily need to meet all the criteria of this clause in order to be considered viable.

- Reproducibility – ability of a particular 3GPP security assurance methodology to produce identical results when applied to the same target at a different time, place, or by a different actor
- Repeatability (or test-retest reliability) – ability of a particular 3GPP security assurance methodology given identical inputs and conditions to produce identical test results
- Ability to model different attacker potentials and different operational environments, allowing traceability and verification of security requirements' sufficiency with respect to attacker/environmental assumptions.
- Current as well as anticipated international recognition – an official acknowledgement and mutual acceptance of a particular 3GPP security assurance methodology as well as its evaluation results by various agencies, consortia, and standard bodies belonging to more than one country. Anticipated international recognition, as well as current international recognition have to be considered when evaluating a particular 3GPP security assurance methodology
- Coordination with other standard bodies – established use or consideration for certification by standard bodies other than 3GPP
- Expandability – ability of a particular 3GPP security assurance methodology to be expanded to a different industry
- Component isolation and ability to reuse pre-certified components – ability to isolate a component of a system for its certification and subsequent re-use as a pre-certified element of another system
- Duration and complexity (cost) of testing cycle – each 3GPP security assurance methodology has anticipated complexity and duration of its testing cycle. In many circumstances, shorter anticipated duration and lower levels of complexity are preferable
- Ability to offer incremental testing, as well as the duration and complexity (cost) of such incremental testing cycle – each 3GPP security assurance methodology might have an anticipated complexity and duration of its testing cycle when an already certified 3GPP product is updated or modified.
- Current as well as anticipated adoption rate – some methodologies have better adoption rate in the telecom industry than others. Anticipated adoption rate, as well as current adoption rate have to be considered when evaluating a particular 3GPP security assurance methodology
- Third party or self-testing options – some methodologies allow self-evaluation and self-declaration by manufacturers, while some other schemes allow only independent, third-party testing by dedicated agents. This property has to be considered when evaluating a particular 3GPP security assurance methodology
- Ability of the 3GPP security assurance methodology to provide measurable results – measurable results of the process is considered to be one of the important properties which has to be considered when evaluating a particular 3GPP security assurance methodology

Editor's note: The use of the word "measurable" is still to be defined.

- Ability of the 3GPP security assurance methodology to allow specifying a set of tests to be performed on the target network products – this possibility is fundamental to verify if security requirements are correctly implemented on the target network products.

- Ability of the 3GPP security assurance methodology to support different assurance levels.

- Ability of the 3GPP security assurance methodology to support different categories corresponding to the desired security baselines for the network products (see 4.5.2.3). The intent of this distinction is for the security objectives to reflect the differing security requirements due, for example, to the exposed or unexposed location of a network product. A network product is to be evaluated for one security baseline or another, but not to be evaluated and certified under multiple different baselines.

Editor's note: Whether it is desirable for a higher security baseline to be inclusive of, and incremental to a lower one is TBD. Such level inclusiveness is to be defined by each methodology.

Editor's Note: Definition of exposed or unexposed location of a network product is FFS.

- Ability of the 3GPP security assurance methodology to focus on the part of the network product which is relevant for the evaluation of the network product according to SECAM (‘scoping of network product').

Editor's Note: It is FFS what is relevant for evaluation according to SECAM, in particular whether it suffices for such an evaluation to evaluate against SASs, or whether the evaluation can go beyond this and consider threats not addressed by any SAS.

- Ability of the 3GPP security assurance methodology to support metrics for measuring and comparing improvement in product security from release to release

- Agility - Ability of the 3GPP security assurance methodology to adapt quickly to new development of attack vectors, tools and techniques.

- Effort, e.g. "time", "money", "human resource", required for the continuous usage and maintenance by 3GPP of the security assurance methodology.

7 Comparison of Proposed Methodologies

Editor's Note: This clause will contain a comparison of the proposed solutions according to the criteria defined in clause 7.

8 Conclusions

8.1 Chosen methodology description

The present study defines the scope and threat model related to security assurance of 3GPP network products (the terminology "network product" is clarified in clause 4.1).

The study introduced two methods (more details can be found in clause 5):

- The first one consists in applying Common Criteria methodology, but not necessarily within the Common Criteria scheme which would require a certification by national Certification Bodies;
- The second one consists in defining a tailored method, but does not prevent the re-use of some Common Criteria notions during the building process.

Methodology 2 is chosen for SECAM. It integrates Common Criteria concepts where efficient and provides the necessary adaptation to 3GPP context where necessary (need to allow accredited self-evaluation, single assurance level and security baseline…)

Editor's Note: the list of differences between methodology 2 and Common Criteria should be expanded to give a full overview of the main differences. Such an overview will prove valuable in 3GPP-internal discussions, when discussing which elements of CC to include in SECAM, and even much more valuable when promoting SECAM to the world outside 3GPP.

- SECAM is built upon an analysis of threats on the considered network products;
- SECAM will follow a Security Assurance process to demonstrate how these threats are covered by tests;
- SECAM will be mainly based on different Security Assurance Specifications, related to a given (set of) network product(s) classe(s), which include security requirements with associated test cases
- SECAM will consider a single security baseline and a single assurance level per network product class for evaluation (see 4.5.2).
    - The security baseline is defined as a set of security requirements and environmental assumptions defining the capacity of the network product(s) to resist a given attack potential. Consequently:
        - each network product can be evaluated only against a single security baseline
        - the security baseline of a network product class cannot be compared to the security baseline of another network product class;
    - SECAM considers a single assurance level per network product class for the evaluation of the security requirements as well as for the vendors' development and lifecycle management process. This means evaluating network products:
        - At constant scope (i.e. a single process will be followed for a given network product class, which will be relevant to this class),
        - At constant depth (which is mainly a black-box approach with occasional and justified usage of grey- or white-box testing),
        - At constant evaluation rigour;
- SECAM assessment will distinguish between
    - Security Compliance testing (see 5.2.4.3),
    - Basic Vulnerability testing (see 5.2.4.4)
    - Enhance Vulnerability Analysis (see 5.2.4.5)
- SECAM will rely on a SECAM Accreditation Body to build trust in the actors of the scheme:

  - The vendor, developing the network product,
  - The security compliance tester, assessing the network product compliance with its SAS,
  - The tools, settings and procedures used for Basic Vulnerability testing

Editor's note: It is FFS which kind of accreditation will be required for Basic Vulnerability testing activity

  - The Enhanced vulnerability analysis tester, assessing whether the network product resists the attacker model defined in the SAS;

- The accredited actors are trusted to undertake the different type of evaluation and SECAM, by the mean of the SECAM Accreditation Body will define a dispute process and revocation process.

8.2 Next steps for the normative phase

Clause 5.2.2 describes the expected content of the methodology building process. SA3 will focus on security compliance and basic vulnerability testing first, in order to improve maturity progressively amongst all partners, before beginning to define Enhanced Vulnerability Analysis. An SAS for security compliance requirements can include requirements on hardening and General Security Testing.

Step 1 (organisational setup)

The methodology building will start with an organizational setup:

- Definition of working way within 3GPP (within SA3, subgroup…)
- Establish way of communication with external group working to prepare accreditation body, e.g. GSMA subgroup

Step 2 (building the pilot SAS, the development and lifecycle requirements and the accreditation requirements)

3GPP will define a first set of SAS for one "pilot" network product class through:

- A consensus on the threats related to the network product
- A consensus on requirements needed to cover these threats,
- Formalization into
  - an SAS including:
  - Security Requirements (including hardening requirements) and the associated test cases
  - Basic Vulnerability Testing activities
  - Development and lifecycle requirements

3GPP may also enter a dialogue with the Accreditation and Conflict Resolution Body on

- accreditation and monitoring rules

Step 3 organisational setup of dry-run

- Agreements with industry partners for a dry-run of "pilot" SAS for one or several network product class(es) (compliance only)
- Definition of confidentiality rules for sensitive information handling
- The accreditation body is invited to join this agreement for the purpose of organising a dry-run for accreditation. Such a joint agreement would usefully contain provisions on sharing knowledge of the dry-run results.

Step 4 (dry run of SAS evaluation and vendor/tester accreditation)

Industry partners will perform a dry-run of the **SAS** evaluation scheme on the basis of the "pilot" SAS from step 2 and the agreement in step 3.

- Evaluate example network products from the selected network product class against the pilot SAS
- 3GPP invites the accreditation body to perform a dry-run for accreditation with the actors such as compliance testers that have volunteered in step 3

Step 5 (SAS finalisation)

Normative workgroup will complete the pilot SASs, using the insight from the dry-run, and turn it into a 3GPP spec

- Correction of assurance, and compliance testing requirements, including hardening and General Security Testing requirements

The normative workgroup and Accreditation and Conflict Resolution Body is invited to also

- refine accreditation and monitoring rules, as well as test methodology and skill requirements for compliance testers, and make the binding rules available to SECAM stakeholders / the public at large

Step 6 (Start of official evaluations)

3GPP will declare the SAS(s) for the selected network product class ready for use in SECAM-compliant evaluations by approving the corresponding specs in SA plenary.

NOTE: SECAM allows that vendor, 3rd party test labs if applicable, and operators use evaluations based on approved SASs according to mutual agreements, independent of the accreditation body.

The Accreditation and Conflict Resolution Body may launch officially accreditations. Actors having performed pilot evaluations, as vendors or compliance testers, may benefit from the fact that some of the dry-run accreditation may be re-used if no change occurred wrt to the final accreditation rules in the relevant part.

NOTE: In parallel to step 6, 3GPP may launch the editing of other SASs

Step 7 (addition of Enhanced Vulnerability Analysis)

Building on experience from the security improvement of the previous evaluations and of their limits, SA3 will launch a new study on addition of Enhanced Vulnerability Analysis into the running evaluation scope to further improve security.

Annex A:
Application of the methodologies

A.1 Application of Methodology 1

A.2 Application of Methodology 2

A.2.1 Basic Vulnerability Testing: examples of test cases

- Requirement name: Port Scanning
  - Requirement reference: BVT-PortScanning
  - Requirement description: Port Scanners reveal open ports. Their output can be used to verify that all running services are explicitly documented and thereby it can be assured that no undocumented or untested service posing a potential security risk is running on the Network Product during operation.
  - Test case:
    - Run port scanner for [protocol] on all external interfaces providing [protocol].
    - Verify that the output of port scans reflects the services documented to be available on the respective interface of the Network Product. Also it needs to be ensured that all services identified by the port scanners are subject to respective tests of other Basic Vulnerability Testing tool categories.
  - Requirement evidences: A document in free form describing: the list of services listening identified on each external interface as well as the pointer in the vendor's documentation describing this service. Derivations between documentation and test must be explained by the Network Product vendor and recorded in this document.
- Requirement name: Vulnerability Scanning
  - Requirement reference**:** BVT-VulnerabilityScanning
  - Requirement description: Vulnerability Scanners check whether known vulnerabilities and other known security shortcomings are present in the tested system. Vulnerability scanners usually check the protocols they are intended for (e.g. TCP/IP and UDP/IP) as well as the services on top of it. Issues identified by those tools usually cover the whole range of possible vulnerabilities.
  - Test case:
    - Run vulnerability scanner for [protocol] on all external interfaces providing [protocol].
    - Perform a Vulnerability Assessment of the issues identified: Evaluate issues according to CVSS score or other suitable scoring mechanisms.
  - Requirement evidences: A document in free form describing: all the identified issues by the tools and their scores. Those issues falling into a medium, high or critical category need to be highlighted and assessed for actual impact in the use case of the Network Product in question.

- Requirement name: Robustness Testing
  - Requirement reference**:** BVT-RobustnessTesting

- Requirement Description**:** Robustness Testing ("fuzzing") tools identify issues in protocols which might occur when unexpected input is provided. Issues identified by those tools could e.g. lead to denial of service vulnerabilities.

- Test case:

  - Run robustness testing tool for [protocol] on all external interfaces providing [protocol].

  - Perform a Vulnerability Assessment of the issues identified: Evaluate issues according to calculated CVSS score or other suitable scoring mechanisms.

- Requirement evidences: A document in free form describing: all the identified issues by the tools and their scores. Those issues falling into a medium, high or critical category need to be highlighted and assessed for actual impact in the use case of the Network Product in question. This could e.g. mean that the testing report states that an unauthenticated remote attacker may force the Network Product to restart by sending certain protocol input.

A.2.2 Security compliance testing: example of security requirements with test cases

NOTE 1: The requirements in this were written using the initial template for security requirements approved at SA3#70. This "old" template is slightly different from the one described in 5.2.2.4.2.3.3 of Methodology 2. The mapping from one template to the other is however straightforward by adding a "threat reference" and splitting "test case" into "Test case" and "Requirement evidences". These requirements will thus not be updated.

A.2.2.1 Network Product Remote Management

Remote management of a 3GPP network product consists of functions, methods and protocols enabling its management from an external device (e.g. a computer located in a different network). The remote management shall be protected and robust against cyber-attacks. If this feature is exploited, it could be difficult for the MNO to recover or stabilize the network. In order to prevent that the Remote Management feature is exploited, some relevant security requirements have been identified and described in the following clauses.

Requirement 1: Traffic Protection

Reference: Remote Management Traffic Protection – RM-TP

Description: All management traffic shall be protected by integrity and encryption; unprotected sessions shall not be accepted. The remote access methods can support natively traffic encryption such as HTTPS, SSHv2 or can be based on lower tunnelling protocol (IPsec VPN, TLS VPN).

The cryptographic algorithm used shall not be affected by known vulnerabilities and crypto-analytic attacks.

Test case:

- Obtain from the Manufacturer details about the algorithms used and compare the list to reference bases of known vulnerabilities
- Verify that plaintext Remote Management sessions are not accepted by the network product

Target network product classe(s): All

Requirement 2: Management Protocols

Reference: Remote Management Protocols – RM-MP

Description: The remote management can support one or more remote access protocol. All the supported protocols shall be robust against known vulnerabilities.

The most secure and robust implementation shall be supported e.g. SSHv2 shall be preferable to SSHv1, SNMPv3 shall be implemented if the management via SNMP trap is supported.

Moreover protocols such as Telnet, SNMPv1 and SNMPv2 shall not be supported as well as FTP. If the network product supports one or more of the above listed protocols, then by default they should be disabled and only enabled by network product administrator.

Test case:

- Obtain from the Manufactures details about the supported protocols and compare the list to reference bases of known vulnerabilities and security threats.
- Verify if the protocols which should be not supported are really unavailable on the target network product. For the protocols which are supposed to be supported, verify that in the default configuration they are disabled (and that can be enabled exclusively by the network product administrator)

Target network product classe(s): All

Requirement 3: IP Restriction

Reference: Remote Management Access IP Restriction – RM-IPRE

Description: The network product administrator shall be able to deploy Access Control Lists (ACLs) on the network product to limit the IP addresses or networks from which the network product can be remotely managed.

Test case:

- Obtain from the Manufacturer details about this feature
- Verify that is not possible to access to the network product from a not allowed IP addresses or networks

Target network product classe(s): All

Requirement 4: User Restriction

Reference: Remote Management Access User Restriction – RM-USRE

Description: The network product administrator shall be able to define on each target network product which users are allowed to perform remote administration and their permissions/privileges.

Test case:

- Obtain from the Manufacturer details about this feature
- Verify that the User Restriction policy is correctly supported and enforced on the target network product

Target network product classe(s): All

Requirement 5: User Authentication

Reference: Remote Management Access User Authentication – RM-USAUTH

Description: Remote access to the target network product shall be granted only to authenticated (remote management) users.

Test case:

- Obtain from the Manufacturer details about this feature
- Verify that unauthenticated access attempts to the target network product are rejected.

Target network product classe(s): All

A.2.2.2 Network Product Local Management

Local management of a target network product consists of functions and methods allowing its management directly through a local connection (e.g. directly from its console). Considering the security of a network product, the local management shall be secure (i.e. authenticated and protected). If this feature is exploited, it could be difficult for the MNO to recover or stabilize the network. In order to prevent that the Network Product Local Management feature is exploited, some relevant security requirements have been identified and described in the following clauses.

Requirement 1: User Authentication

Reference: Local Management Access User Authentication – LM-USAUTH

Description: Local access to the target network product shall be granted only to authenticated (local management) users.

Test case:

- Obtain from the Manufacturer details about this feature
- Verify that unauthenticated access attempts to the target network product are rejected

Target network product classe(s): All

Requirement 2: Strong User Authentication

Reference: Local Management Strong Authentication – LM-SUSAUTH

Description: The user allowed to access the network product via console (i.e. directly through a local connection) shall be authenticated using a strong multifactor authentication mechanism based on PIN + One Time Password (OTP), smartcards and/or biometrics elements.

Test case:

- Obtain from the Manufacturer details about this feature
- Verify if the Strong User Authentication policy is implemented and enforced on the target network product (e.g. if management users attempting to authenticate themselves to the target network product with traditional "username and password" scheme are rejected).

Target network product classe(s): Exposed

Requirement 3: User Restriction

Reference: Local Management Access User Restriction – LM-USRE

Description: The network product administrator shall be able to define on each target network product which users are allowed to perform local administration and their permissions/privileges.

Test case:

- Obtain from the Manufacturer details about this feature
- Verify that the User Restriction policy is correctly supported and enforced on the target network product.

Target network product classe(s): All

A.2.2.3 Password Management

Passwords can control access to resource of the network product or to the network product itself. This is accomplished through the definition of a secret allowing to authenticate and authorize the requests to the target network product. When a request is received, by the target network product the request is challenged for password and identity verification. Depending on the result of the verification process, the access can be granted, denied or limited. For security best practice, for all users an external authentication server (AAA) should be preferred. Locally configured password shall be still configured in the case of a server or network failure, but the network product can also have other passwords/secrets within its configuration (e.g. NTP key, SNMP community string and so on), so the problem of password management is fundamental even if an external AAA server is used. In order to prevent that the Password Management feature is exploited, some relevant security requirements have been identified and described in the following clauses.

Requirement 1: External Authentication Server

Reference: Password Management External Authentication Server – PM-EXTAUTHSRV

Description: As security best practice, passwords should be managed by external authentication server based on Radius or Diameter protocols.

Test case:

- Obtain from the Manufacturer details about this feature
- Verify that the feature is effectively supported.

Target network product classe(s): All

Requirement 2: Local Password Storage

Reference: Password Management Local Storage – PM-LS

Description: Password/secret stored locally in the network product shall be protected using strong algorithms.

Test case:

- Obtain from the Manufacturer details about this feature

- Verify that the algorithms used to store the secrets within the target network product are robust and not vulnerable to known attacks (e.g. password recovering using brute force attacks shall not be possible).

- If passwords are locally stored in the target network product using hash functions, verify that SHA-256 or SHA-1 is used (and that MD5 is not used).

- If passwords are locally stored using encryption algorithm, check that this encryption algorithm is not vulnerable to known crypto-attacks.

Target network product classe(s): All

Requirement 3: Password Lockout

Reference: Password Lockout – PM-PLO

Description: The network product shall detect repeated invalid attempts to sign into an account with incorrect passwords during a short period of time to lock out the user's account and prevent further attempts, at least for a certain period of time. If N invalid attempts to login to the same account are made during an interval of Tdetect minutes, then the account is disabled for Tlockout minutes (after that period lockout is cleared).

While this mechanism is effective against concerted attacks against a single account, it does nothing to prevent an intruder from simultaneously trying to guess the passwords of many users. A more sophisticated mechanism might extend this as follows: If M invalid login attempts are made from network address A, to any account, during an interval of Tdetect minutes, then the address A is disabled for Tlockout minutes.

The parameters N, M Tdetect and Tlockout shall be set to default values which can be set and changed exclusively by the network product administrator.

This mechanism shall be applied only to users, exempting at least one administrator login. This limits the scope of denial of service attacks.

Test case:

- Obtain from the Manufacturer details about both features

- Verify that the set values for N, M, Tdetect and Tlockout are properly handled after failed login attempts (e.g. accounts are blocked after N failed attempts).

Target network product classe(s): All

Requirement 4: No Service Password Recovery

Reference: No service password recovery– PM-NSPR

Description: Many network devices have a function that resets the current system password (password recovery). This function shall be disabled. If this is not possible, it shall be ensured that an attacker cannot gain access to the configuration of the network device. For this, the entire configuration of the network device shall be irretrievably deleted in the event that the system password is reset.

Test case:

- Obtain and verify documentation on the password recovery procedures for the target network product.

- Verify that this functionality is disabled or if it is enabled check that the entire configuration of the network device was irretrievably deleted.

Target network product classe(s): All

Requirement 5: No Blank Password

Reference: No blank password– PM-NBP

Description: It shall be impossible configure blank local passwords. Note that when an external authentication server is used, a policy preventing the configuration of blank passwords on the external authentication server should be implemented.

Test case:

- Obtain and verify documentation on this feature for the target network product
- Verify that local blank passwords cannot be configured on the target network product

Target network product classe(s): All

Requirement 6: Enforce Password History

Reference: Password history – PM-EPH

Description: The network product shall support the possibility to determine the number of unique new passwords that have to be associated with a user account before an old password can be reused. This policy enables administrators to enhance security by ensuring that old passwords are not reused continually. This mechanism should be applied to all user accounts configured on the network product.

Test case:

- Obtain and verify documentation on the password recovery procedures
- Verify that when this feature is enabled, it is not possible to reuse old passwords.

Target network product classe(s): All

Requirement 7: Enforce Strong Passwords

Reference: Enforce Strong Passwords– PM-ESP

Description: The network product shall support the possibility to define password policy so that all user accounts are protected with strong passwords. This policy should be enabled by default with a default rule.

Test case:

- Obtain and verify documentation on the password recovery procedures
- Verify if it is possible to configure password not matching the defined policy.

Target network product classe(s): All

Requirement 8: Enforce Password Expiration

Reference: Enforce Password Expiration – PM-EPE

Description: Although a strong password can help protect against intruders, it is possible to eventually guess or steal the password of a resource. For this reason, passwords should be changed periodically to minimize damages when a password is compromised without the user's knowledge. The network product shall support the possibility to define a password expiration policy for all user accounts. This policy should be enabled by default with a default value.

Test case:

- Obtain and verify documentation on the password recovery procedures
- Verify if passwords expires after the configured period of validity.

Target network product classe(s): All

A.2.2.4 Software

Software bugs can introduce vulnerabilities which can be exploited by an attacker to breach the network product (for example to gain root privileges). Software bugs stem generally from an insecure/poor application design, an insecure code developing, improper flaws and can fall into a fairly small number of broad categories which include memory safety (e.g. buffer overflow and dangling pointer bugs), race condition, secure input and output handling, faulty use of an API, improper use case handling, improper exception handling, pre-processing input strings after they are checked for being acceptable, etc. In order to prevent that the unsecure, vulnerable software is exploited, some relevant security requirements have been identified and described in the following clauses.

Requirement 1: Patching

Reference: Patching – S-PA

Description: Information on publicly known vulnerabilities in various software/operating system is freely accessible on Internet (http://cve.mitre.org/cve/, http://www.securityfocus.com/vulnerabilities). The operating system/main applications used within the target network product shall embed all patches for known vulnerabilities at the date of delivery.

Test case:

- Obtain from the Manufacturer and verify documentation on all the patches that were applied to the Operating System/main applications of the target network product to close known security issues
- Compare this list to reference bases of known vulnerabilities (http://cve.mitre.org/cve/, http://www.securityfocus.com/vulnerabilities)
- Use automatic tools like Nessus to make a Vulnerability Assessment of the network product

Target network product classe(s): All

Requirement 2: Secure Software Development

Reference: Secure Software Development – S-SSWD

Description: Software assurance/secure code analysis tools to identify and fix buffer overflows, memory leaks shall be used by manufactures to reduce bugs stem from code development errors.

Test case:

- Obtain from the Manufacturer evidences about the results of this assurance
- Test the network product using unexpected input (e.g. fuzzy inputs)

Target network product classe(s): All

Requirement 3: Secure Protocol Stack Development

Reference: Secure Protocol Stack Implementation – S-SPSD

Description: Protocol stack development shall be made robust against manipulation and unexpected inputs. This can be achieved, e.g. by verifying the validity of the values transferred in fields, parameters, etc. Typical implementation errors include:

- No validation on the lengths of transferred data
- Incorrect assumptions about data formats
- No validation that received data complies with the specification
- Insufficient handling of protocol errors in received data
- Insufficient restriction on recursion when parsing complex data formats

Test case:

- Obtain and verify documentation about secure software development cycle and testing (fuzzing/load) that was put in place for the development or integration of the different protocol stacks particularly for the telecom specific protocols
- Conduct load and fuzz testing for the different stacks

Target network product classe(s): All

Requirement 4: Secure System Patching

Reference: Secure system patching – S-SSP

Description: The network product should support the possibility to prevent illegal software patching.

Test case:

- Obtain and verify documentation on the security environment of the network product

Target network product classe(s): Exposed

Requirement 5: Secure System Software Revocation

Reference: Secure system software revocation – S-SSSR

Description: Once the software image is legally updated, rolling-back to a previous potentially exploitable software image should be granted only to administrator.

Test case:

- Obtain and verify documentation on the security environment of the network product
- Verify the software rollback procedure

Target network product classe(s): Exposed

A.2.2.5 System Secure Execution Environment

The target network product shall implement a secure execution environment, intended as a system environment where sensitive operations (e.g. encryption/decryption of user data) and data are securely implemented and executed. This security environment is achieved if the system is securely hardened. In the following clauses some relevant security requirements to enable a secure execution environment have been identified and described.

Requirement 1: Removal of Unnecessary Service

Reference: Unnecessary Service Removal – SSEE-RUS

Description: Target network product shall support just those running services/protocols (httpd, mysqld etc…) that are necessary for the network product functionalities.

Test case:

- Obtain from the Manufacturer the list of supported services
- Access to the network product and verify the list of the enabled service (e.g. by means of an appropriate command)
- Use automatic port scan tools like Nessus to check active services.

Target network product classe(s): All

Requirement 2: Unused Interfaces Disabling

Reference: Unused physical interfaces disabling – SSEE-UID

Description: In most cases, all available interfaces of a network product, including those that are not used, are enabled by default at system start. Interfaces which are not in use shall be permanently disabled so that they remain inactive even in the event of a reboot.

Test case:

- List all the physically accessible interfaces of the network product (outside and inside of the chassis)
- Obtain and verify documentation on the activation/de-activation of all these interfaces
- Test that these interfaces are effectively electrically disabled and that no service or data is accessible through them

Target network product classe(s): All

Requirement 3: Restricting System Boot Source

Reference: Restricting system boot source– SSEE-RSBS

Description: Many network products allow an operating system to be booted from another source (e.g., USB flash drive, memory card). A target network product shall be configured in such a way that only the intended operating system can boot and that it can boot only from the internal memory. Alternatively, interfaces (USB, card slots, etc.) potentially allowing an external operating system to be booted shall be disabled.

Test case:

- List all the physically accessible interfaces of the network product (outside and inside of the chassis)
- Obtain and verify documentation on the activation/de-activation of all these interfaces
- Test that these interfaces are effectively electrically disabled and that no service or data is accessible through them

Target network product classe(s): All

Requirement 4: Unsecure Protocol Disabling

Reference: Unsecure protocol disabling – SSEE-UPD

Description: Unsecure or vulnerable protocols such as Telnet, SNMPv1 and SNMPv2 shall not be supported as well as ftp. If the target network product supports one or more of the above-listed protocols, then by default they shall be disabled and they can only be enabled by the network product administrator.

Test case:

- Use automatic tool such as Nessus to verify if these protocols are disabled.

Target network product classe(s): All

Requirement 5: Key Material Access Rules

Reference: Key material access rules– SSEE-KMAR

Description: It shall not be possible from unauthorized access to get keying material shared between the target network product and currently active User Equipment connected with it, or to get access to the keying material with which the IPsec connection (when used) to the core network products or other elements of the core network are protected.

Test case:

- Obtain and verify documentation on the security environment of the target network product
- Keys stored inside the target network product shall never leave a secure environment within the network product itself. Verify how the keys are protected.
- Verify that only authorised access are granted to the secure environment, i.e. to data stored and used within, and to functions executed within.

Target network product classe(s): eNodeB, MME/SGSN

Requirement 6: Secure System Boot

Reference: Secure system boot – SSEE-SSB

Description: The target network product should support the possibility to verify software image integrity at boot time, detecting, for example, software image tampering and/or unauthorized software image updates.

Test case:

- Obtain and verify documentation of this feature on the target network product
- The integrity of a software component is typically verified by comparing the result of a measurement (typically a cryptographic hash) of the component to the expected reference value, usually provided by the manufacture. If these values match, the component is successfully verified and it can be started
- Verify that the cryptographic algorithms used to calculate the hash is not vulnerable to known attacks.

Target network product classe(s): All

Requirement 7: Secure Time Synchronization

Reference: Secure time synchronization – SSEE-STS

Description: Clock synchronization with a time server is a critical middleware service enabling several services on a 3GPP network product, for example accurate and secure localization, digital certificate verification and thus for the establishment of secure links. These benefits could make clock synchronization protocols a prime target of malicious adversaries who want to disrupt the legal operation of the network product.

Test case:

- Obtain and verify documentation on the security environment of the network product
- Verify how the mechanism has been implemented and if it vulnerable to know attacks

Target network product classe(s): Exposed

A.2.2.6 Network Services

Preventing suspicious network traffic from reaching a certain network product is a fundamental way to minimize the risk of several cyber-attacks (e.g. DoS attacks). In order to prevent that Network Services feature is exploited, some relevant security requirements have been identified and described in the following clauses.

Requirement 1: Traffic Filtering

Reference: Traffic Filtering – NS-TF

Description: One of the fundamental functions of network products is the control of data traffic on the basis of the IP destination and sender addresses as well as the used ports and protocol status. A network product shall therefore support filters (e.g., access control lists, local firewall, etc.) to regulate incoming and outgoing traffic on the basis of address information, services (ports) and protocol statuses and types. These can be used to route packets through the network device as well as to accept or reject packets sent to one of the network product's addresses on the basis of defined criteria.

Test case:

- Obtain and verify documentation on local inbound/outbound filters for the network product
- Verify that after applying filtering rules on specific ports/protocols/interfaces (for example on IPsec and SSH traffic allowed as inbound traffic) that these rules are effectively enforced

Target network product classe(s): All

Requirement 2: IP Anti-Spoofing

Reference: IP Anti-Spoofing – NS-IPAS

Description: This type of attack allows a host, application or a malicious network product to mimic the actions of a genuine network product. Typically the attacker pretends to be an innocent host by reusing its IP addresses in network packets. In order to protect against this type of attack the target network product should implement anti-spoofing mechanisms, e.g. to reject packet with invalid source addresses, coming from unexpected interface, etc...

Test case:

- Obtain and verify documentation on this feature
- Verify that spoofed packets are rejected

Target network product classe(s): All

Requirement 3: Tunnelling in GTP

Reference: GTP Tunnelling – NS-GTPTN

Description: This attack could pose a moderate security threat. It may be possible for attackers to wrap attack traffic in GTP Version 0 or 1 Packet, which has another embedded GTP Packet as part of its payload. As GTP is used to encapsulate packets originating from a mobile station, it is possible for a mobile station to create a GTP packet and forward it along to the SGSN.

Upon receiving the GTP packet, the SGSN will encode it again, and forward it to the GGSN, through the relative PDP context. This embedded GTP packet may be potentially decoded via the GGSN and forwarded into the GGSN infrastructure, or decoded a second time, allowing an attacker to spoof GTP packets coming from a range of different answers. Another potential attack would be attackers sending recursive GTP packets, which is a GTP packet that contains X number of other GTP packets embedded within.

Test case:

- Examine incoming packet for possible exploitation code in the embedded GTP data fields.

Target network product classe(s): MME/SGSN, GGSSN

A.2.2.7 3GPP Capability Configuration

Preventing unsecure configurations deployment of 3GPP features can be a fundamental way forward to minimize the risk of several cyber-attacks. In order to prevent that the Configuration Security feature is exploited, some relevant security requirements have been identified and described in the following clauses.

Requirement 1: Security Algorithm Modification

Reference: Security Algorithm Modification – CC-SAM

Description: It shall not be possible from unauthorized access, to modify security algorithms supported by the target network product, e.g. to perform a downgrade attack by configuring the use of a weaker algorithm.

Test case:

- Verify that the security algorithm configuration cannot be modified from unauthorized users.

Target network product classe(s): eNodeB, MME/SGSN

Requirement 2: Only EIA0

Reference: Only EIA0– CC-OEIA0

Description: It shall not be possible to configure just EIA0 on the target network product. EIA1 and/or EIA2 shall be enabled in compliance to the specification requirements that demand the use of integrity as mandatory and the use of EIA0 only for non-authenticated emergency services

Test case:

- Verify that a configuration where only EIA0 is enabled it is not accepted on the target network product as valid. Verify that it is also needed to enable at least one of the other types of algorithms that are different from the "Null Integrity".

Target network product classe(s): eNodeB, MME/SGSN

Requirement 3: Integrity Algorithms Disabling

Reference: Integrity Algorithms Disabling – CC-IAD

Description: Each target network product shall be configured via network management with lists of algorithms which are allowed for usage. There shall be one list for integrity algorithms and one for ciphering algorithms. These lists shall be ordered according to a priority decided by the operator. When a security context is established for an authenticated user, the target network product shall choose from its configured list the algorithms which have the highest priority and that are also supported on the terminal side. (UE EPS security capabilities). In the case where the target network product is configured to require the use of only EIA0 (NULL Integrity) as integrity algorithm the target network product shall not allow the user to connect to the network even if the user is successful authenticated and EIA0 is the only integrity algorithm that match in the target network product and terminal configuration. By allowing the user to connect to the

network the mandatory integrity requirement for signalling protection is not respected. The use of EIA0 shall be allowed only for unauthenticated emergency calls.

Test case:

- Obtain and verify documentation about integrity algorithms supported on the target network product.
- Check that EIA1 and EIA2 are supported as a standard feature.
- Verify the configuration of the algorithms list on the target network product
- Testing the network products behaviour in the case where "erroneously "only EIA0 (NULL Integrity) is enabled on the target network product.

Target network product classe(s): eNodeB, MME/SGSN

A.2.2.8 Network Product Access Control

Network product access control consists of rules restricting the access to the network product (i.e. user authentication and authorization). In order to prevent that the Network Product Access feature is exploited, some relevant security requirements have been identified and described in the following clauses.

Requirement 1: User Profiling/User Authorization

Reference: User Profiling - NAC-UP

Description: Several users with different privileges shall be defined

Test case:

- Verify if different user profiles can be identified for example administration profile, visualization profile
- Verify if the different profiles are correctly applied

Target network product classe(s): All

Requirement 2: No Default Users

Reference: No default users - NAC-NDU

Description: Default users with default passwords shall not be allowed

Test case:

- Verify if default users are disallowed.

Target network product classe(s): All

Requirement 3: No Disable User Authentication

Reference: No disable user authentication - NAC-NDUA

Description: User authentication cannot be disabled on the target network product.

Test case:

- Verify user authentication cannot be disabled.

Target network product classe(s): All

A.2.2.9 User Audit of Network Product

Auditing is the practice of inspecting logs for the purpose of verifying that the system is in a desirable security state or to answer questions about how the system arrived at a particular state. In order to prevent that the User Audit of network product feature is exploited, some relevant security requirements have been identified and described in the following clauses.

Requirement 1: User Activity Audit

Reference: User activity accountability for system audit UANP-UACC

Description: User undertaking audit of network product activities can get access to sensitive information. This should be restricted to a certain subset of users.

Test case:

- Verify user authentication for undertaking network product audit cannot be disabled and is correctly enforced by the audited product.

Target network product classe(s): All

Annex B:
Common criteria overview

B.1 Target audience of the CC

There are mainly three groups with a general interest in evaluation of the security properties of Target of Evaluations (TOEs). They are as follows:

a) Consumers: Consumers can use the results of CC evaluations to help decide whether a TOE (Information and Communications Technology (ICT) product) fulfils their security needs. Consumers can also use the evaluation results to compare different TOEs. The CC gives consumers, especially in consumer groups and communities of interest, an implementation-independent structure, termed the Protection Profile (PP), in which to express their security requirements in an unambiguous manner.

b) Developers: The CC is intended to support developers in preparing for and assisting in the evaluation of their TOEs and in identifying security requirements to be satisfied by those TOEs. These requirements are contained in an implementation-dependent construct termed the Security Target (ST). This ST may be based on one or more PPs to show that the ST conforms to the security requirements from consumers as laid down in those PPs. The CC can then be used to determine the responsibilities and actions to provide evidence that is necessary to support the evaluation of the TOE against these requirements. It also defines the content and presentation of that evidence.

c) Evaluators: The CC contains criteria to be used by evaluators when forming judgments about the conformance of TOEs to their security requirements. The CC describes the set of general actions the evaluator is to carry out.

d) Others: Auditors (internal and external), Security architects and designers, system security officers, etc

B.2 CC and the ISO/IEC

The CC has been adopted and published by the International Organization for Standardization/ International Electro-technical Commission (ISO/IEC), following earlier attempts to integrate information technology and computer security criteria by various regional SDO's.

By the ISO/IEC-developed Standards, the CC is composed of three parts (see Brief History of the Common Criteria: http://www.niap-ccevs.org/cc_docs/); these parts or documents are used by the certifying body of a CC scheme and the evaluation facilities. Brief explanation of each document is given below

a) ISO/IEC 15408-1:2009: Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model:
ISO/IEC 15408-1:2009 establishes the general concepts and principles of IT security evaluation and specifies the general model of evaluation given by various parts of ISO/IEC 15408 which in its entirety is meant to be used as the basis for evaluation of security properties of IT products.
It provides an overview of all parts of ISO/IEC 15408. It describes the various parts of ISO/IEC 15408; defines the terms and abbreviations to be used in all parts ISO/IEC 15408; establishes the core concept of a Target of Evaluation (TOE); the evaluation context; and describes the audience to which the evaluation criteria are addressed. An introduction to the basic security concepts necessary for evaluation of IT products is given. It defines the various operations by which the functional and assurance components given in ISO/IEC 15408-2 and ISO/IEC 15408-3 may be tailored through the use of permitted operations. The key concepts of protection profiles (PP), packages of security requirements and the topic of conformance are specified and the consequences of evaluation and evaluation results are described. ISO/IEC 15408-1:2009 gives guidelines for the specification of Security Targets (ST) and provides a description of the organization of components throughout the model. General information about the evaluation methodology is given in ISO/IEC 18045 and the scope of evaluation schemes is provided.

b) ISO/IEC 15408-2:2008: Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional components:
ISO/IEC 15408-2:2008 defines the content and presentation of the security functional requirements to be assessed in a security evaluation using ISO/IEC 15408. It contains a comprehensive catalogue of predefined security functional components that will meet most common security needs of the marketplace. These are organized using a hierarchical structure of classes, families and components, and supported by comprehensive user notes. ISO/IEC 15408-2:2008 also provides guidance on the specification of customized security requirements where no suitable predefined security functional components exist.

c) ISO/IEC 15408-3:2008: Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 3: Security assurance components:
ISO/IEC 15408-3:2008 defines the assurance requirements of the evaluation criteria. It includes the evaluation assurance levels that define a scale for measuring assurance for component targets of evaluation (TOEs), the composed assurance packages that define a scale for measuring assurance for composed TOEs, the individual assurance components from which the assurance levels and packages are composed, and the criteria for evaluation of protection profiles and security targets.
ISO/IEC 15408-3:2008 defines the content and presentation of the assurance requirements in the form of assurance classes, families and components and provides guidance on the organization of new assurance requirements. The assurance components within the assurance families are presented in a hierarchical order.

There is also an accompanying document ISO/IEC 18045:2008:

d) ISO/IEC 18045:2008: Information technology -- Security techniques -- Methodology for IT security evaluation:
ISO/IEC 18045:2008 is a companion document to ISO/IEC 15408, Information technology - Security techniques - Evaluation criteria for IT security. ISO/IEC 18045:2008 defines the minimum actions to be performed by an evaluator in order to conduct an ISO/IEC 15408 evaluation, using the criteria and evaluation evidence defined in ISO/IEC 15408. ISO/IEC 18045:2008 does not define evaluator actions for certain high assurance ISO/IEC 15408 components, where there is as yet no generally agreed guidance.

B.3 Common Criteria (Technical) Process overview

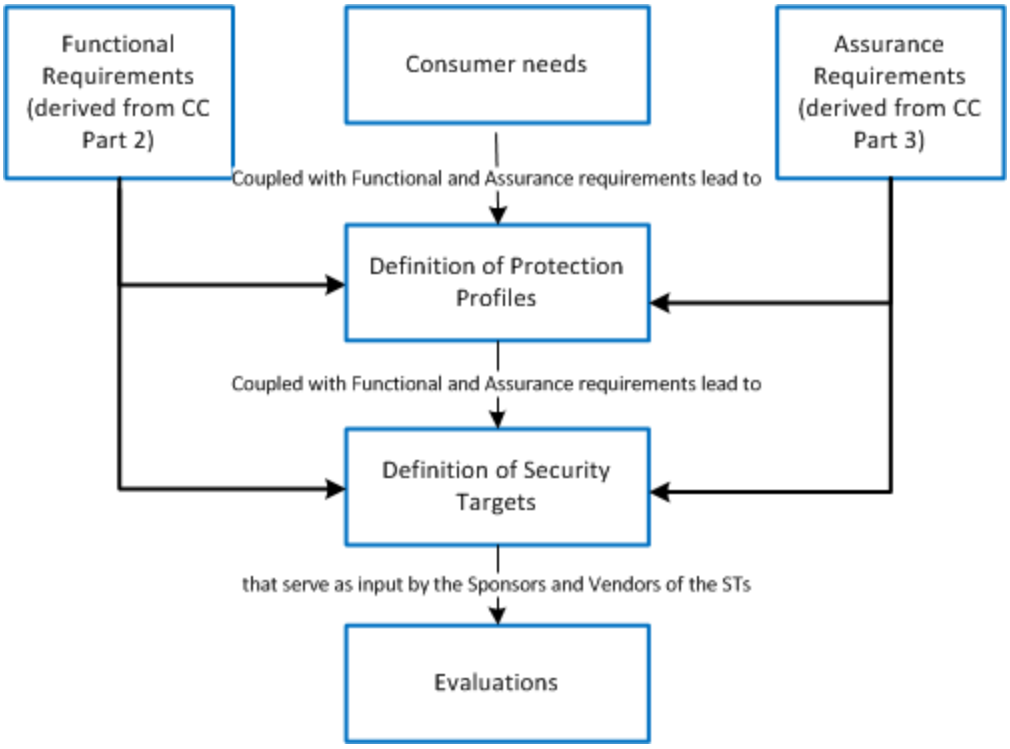


Figure B.3-1. Overview of the CC Technical Evaluation process [8].

Referring to Figure B.3-1, the Common Criteria approach to the overall evaluation process is broadly divided into three stages as follows:

a) The Development Stage

In this stage, the CC defines a set of IT requirements of known validity which can be used in establishing security requirements for a network product. For a network product, such requirements can be derived from Third Generation Partnership Project (3GPP) Specifications pertaining to it, such as 3GPP TS 33.401 [8], TS 33.402 [9], TS 23.401 [10], TS 23.402 [11], etc. The CC also defines the Protection Profile (PP) construct which allows prospective network product manufacturers (or developers) to create standardized sets of security requirements for a network product -PP which will meet their needs. The Target of Evaluation (TOE) (a mobile network product, for our case) is that part of the product or system which is subject to evaluation. The TOE security threats, objectives, requirements, and summary specification of security functions and assurance measures together form the primary inputs to the Security Target (ST). The PP is transformed into ST and is used by the evaluators as the basis for evaluation of a network product.

b) The Evaluation Stage

The principal inputs to evaluation are the Security Target, the set of evidence about the TOE (a mobile network product, for our case) and the TOE itself. The expected result of the evaluation process is a confirmation that the ST is satisfied for the TOE, with one or more reports documenting the evaluation findings.

The Common Evaluation Methodology (CEM) [13] document describes the evaluation process that consists of the evaluator performing the evaluation input task, the evaluation output task and the evaluation sub-activities.

c) The Operation Stage

Once a TOE (mobile network product, for our case) is in operation vulnerabilities may surface, or environmental assumptions may require revision. Reports may then be made to the developer requiring changes to the TOE. Following such changes re-evaluation may be required.

Annex C:
Self-evaluation and Self-evaluation with Third-party Certification Analysis

As shown in clause 4.5.2 and figure 4.5.2.3-1 copied below, the vendor can take the Evaluator role and issue a self-declaration; this is what sometimes referred to as "self-certification"", but for clarity of definitions, this term is not used in the present document. The Certification Authority role can be taken by an independent entity, e.g., GSMA, NVIOT or CCRA, which would in this case be a third-party certification.

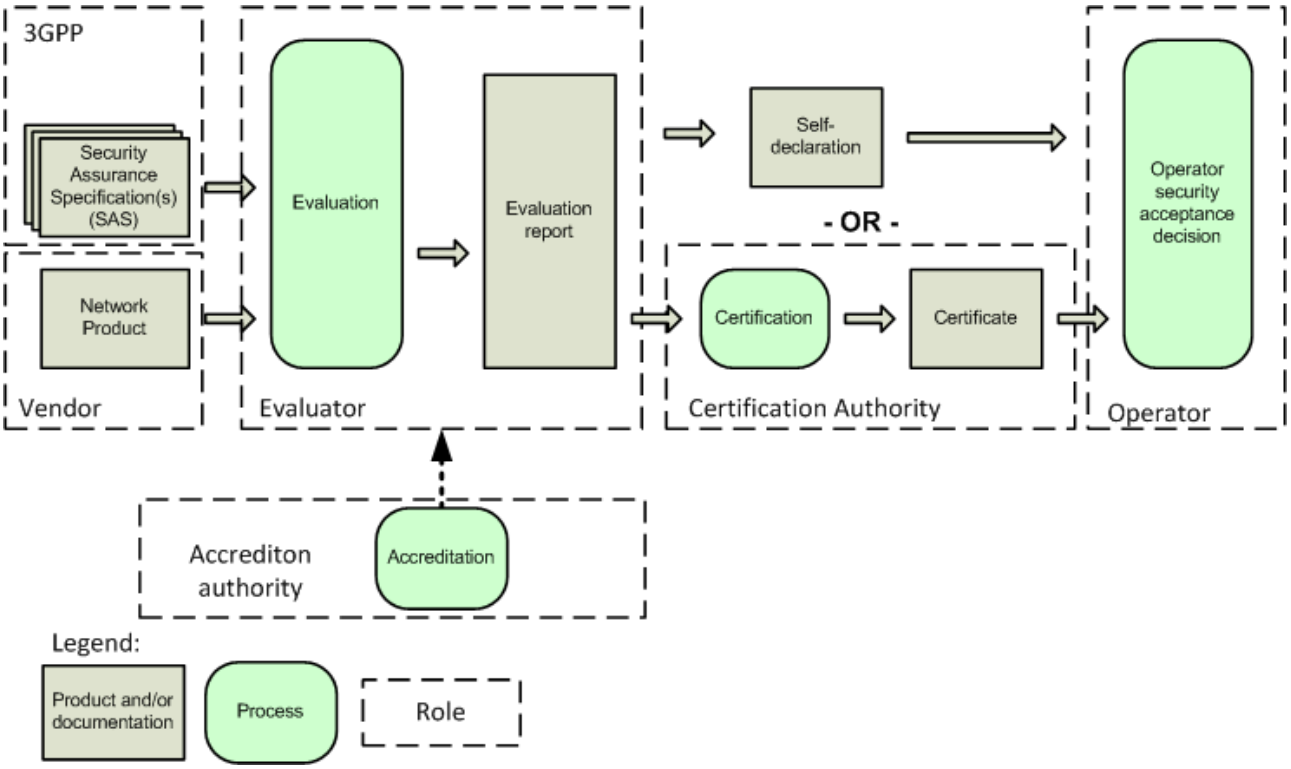


**Figure 4.5.3.1-1 Roles involved in the security assurance process.
The text "- OR –" in the figure indicates that the evaluation report may be provided directly to the operator or that it may be subject to certification first.**

As it can be seen on the diagram above, the self-declaration step corresponds to giving directly the self-evaluation report from the vendor to the operator. So the wording "self-certification" is a synonym to "self-evaluation" plus self-declaration. As this wording is not used anywhere else in the Security Assurance world, it is proposed not to use the wording "self-certification" anymore in the TR to avoid confusion.

The following text and table will clarify the differences between "self-evaluation" plus self-declaration (formerly called self-certification) and self-evaluation with third party certification of the evaluation results.

(1) Should supporting certification be a criterion for evaluation of methodologies?

Some methodologies can support third-party certification; other methodologies support only self-evaluation without certification of the results. In order to select the methodology, supporting certification should be a criterion since it will impact the methodology selection.

(2) Should self-evaluation be a requirement for all methodologies?

Not all existing methodologies accept self-evaluation. For example, when the CCRA recognition is needed, the CC framework only supports third-party evaluation and certification. Thus methodologies that only support third-party certification will be excluded if self-evaluation is a requirement.

Therefore support of self-evaluation should not be a requirement for evaluation of the methodologies.

(3) What is the difference between self-evaluation and self-evaluation with third party certifications?

The analysis of the two approaches considers the following dimensions: certification authority, time and cost effectiveness, confidence of assurance level.

NOTE: This analysis is not intended to value self-evaluation based methodologies or self evaluation + third-party certification based methodologies but to look at what the trade-off in terms of cost, time and assurance level is, in case there is a third party certification at the end of the process or not.

The analysis is as follows:

N°	Dimension	Self-evaluation plus self-declaration	Self-evaluation + Third-party certification
1	Certification Authority	None	Authorized existing certification authorities (e.g., GSMA, NVIOT or CCRA
2	Time and cost for certification	Not applicable	The third-party certification authority needs and to be able to decide if the evaluation report gives sufficient evidence that a proper evaluation of the network product has been conducted. Cost and time is increased due to the third-party certification, but can be fixed as the evaluation is carried out by the vendor.
3	Confidence of assurance level	The assurance level can be abused. More confidence in the assurance level can be achieved if the methodology mandates accreditation of the evaluator in order to demonstrate they have the skills, working practices and resources to conduct the evaluation (e.g. using quality/security standard ISO 17025, etc.)	High confidence in compliance with the assurance level.

It can be seen from the above table that addition of third-party certification at the end of the process provides a higher confidence of the assurance level but increases time and cost.

Annex D:
Threat modelling frameworks

D.1 ITU-T X.805

D.1.1 Overview

The following presentation given at IETF 63 (2005) provides a good overview of application of ITU-T X.805 in practice: http://www.ietf.org/proceedings/63/slides/saag-3/saag-3.ppt

X.805 used the ITU-T X.800 threat model which is an Attacker-centric threat model considering 5 types of security threats against the network products to violate the Confidentiality, the Integrity and the Availability (CIA) of data and services:

- Destruction: Destruction of information and/or other resources (attack on availability)
- Corruption: Corruption or modification of information (attack on integrity)
- Removal: Theft, removal or loss of information and/or other resources (attack on availability)
- Disclosure: Disclosure of information (attack on confidentiality)
- Interruption: Interruption of services (attack on availability)

It also provides the following 8 security dimensions aiming to address all possible network product vulnerabilities:

- Access Control: methods to limit and control access to network elements, services & applications (e.g. password, ACL, firewall);
- Authentication: methods to provide Proof of Identity (e.g. shared secret, PKI, digital signature, digital certificate);
- Non-repudiation: mechanisms to prevent the ability to deny that an activity on the network occurred (e.g. system logs, digital signatures);
- Data Confidentiality: mechanisms to ensure confidentiality of data (e.g. encryption);
- Communication Security: methods to ensure information only flows from source to destination (e.g. VPN, MPLS, L2TP);
- Data Integrity: methods to ensure data is received as sent or retrieved as stored (e.g. MD5, digital signature, anti-virus software);
- Availability: methods to ensure network elements, services and application available to legitimate users (e.g. IDS/IPS, network redundancy, BC/DR);
- Privacy: methods to ensure that the identification, the network use is kept private (e.g. NAT, encryption).

Table D.1.1-1: How the Security Dimensions map to the Security Threats

Security Dimension	X.800 Security Threats				
	Destruction	Corruption	Removal	Disclosure	Interruption
Access Control	X	X	X	X	
Authentication			X	X	
Non-Repudiation	X	X	X	X	X
Data Confidentiality			X	X	
Communication Security			X	X	
Data Integrity	X	X			
Availability	X				X
Privacy				X	

D.1.2 Security layers and security planes

X.805 also uses the concept of security layers and security planes as key concepts to further structure the threat assessment.

D.1.2.1 Security layers

X.805 defines three security different layers as show in figure 2: Infrastructure, Service and Applications. Each Security Layer has unique vulnerabilities and threats. The goal of the mapping is determining how the elements in the upper layer can rely on protection that lower layers provide (i.e. determine how infrastructure security enables services security and how this latter, in turn, enables applications security).

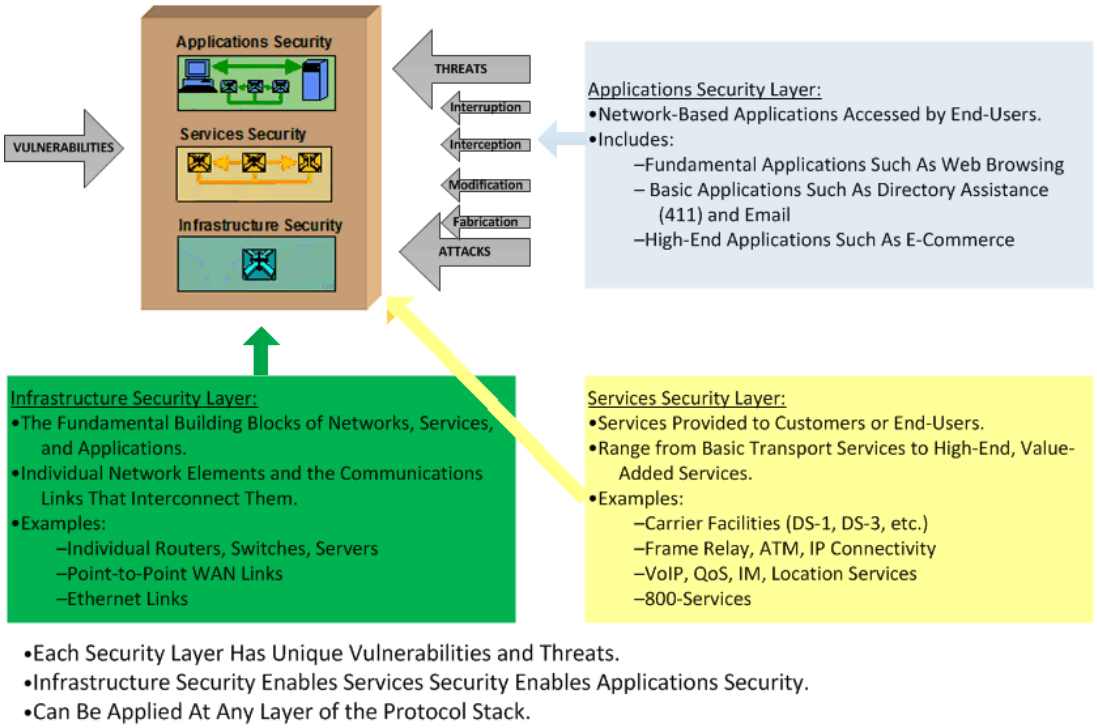


Figure D.1.2.1-1: Security Layers

A concrete application on of these Security Layers to IP Networks could be the following:

Infrastructure Security Layer

- Individual routers, servers (3GPP network products)
- Communication links

Services Security Layer

- Basic IP transport
- IP support services (e.g., AAA, DNS, DHCP)
- Value-added services: (e.g., VPN, VoIP, QoS)

Applications Security Layer

- Basic applications (e.g. FTP, web access)
- Fundamental applications (e.g., email)
- High-end applications (e.g., e-commerce, e-training)

The applications and services which serve the function of a 3GPP network product (for example OAM management application of an MME or basic IP transport for the communication links) are in the scope.

D.1.2.2 Security planes

X.805 defines three security planes (Management Security Plane, Control/Signalling Security Plane and End-User Security Plane) as show in the figure below:

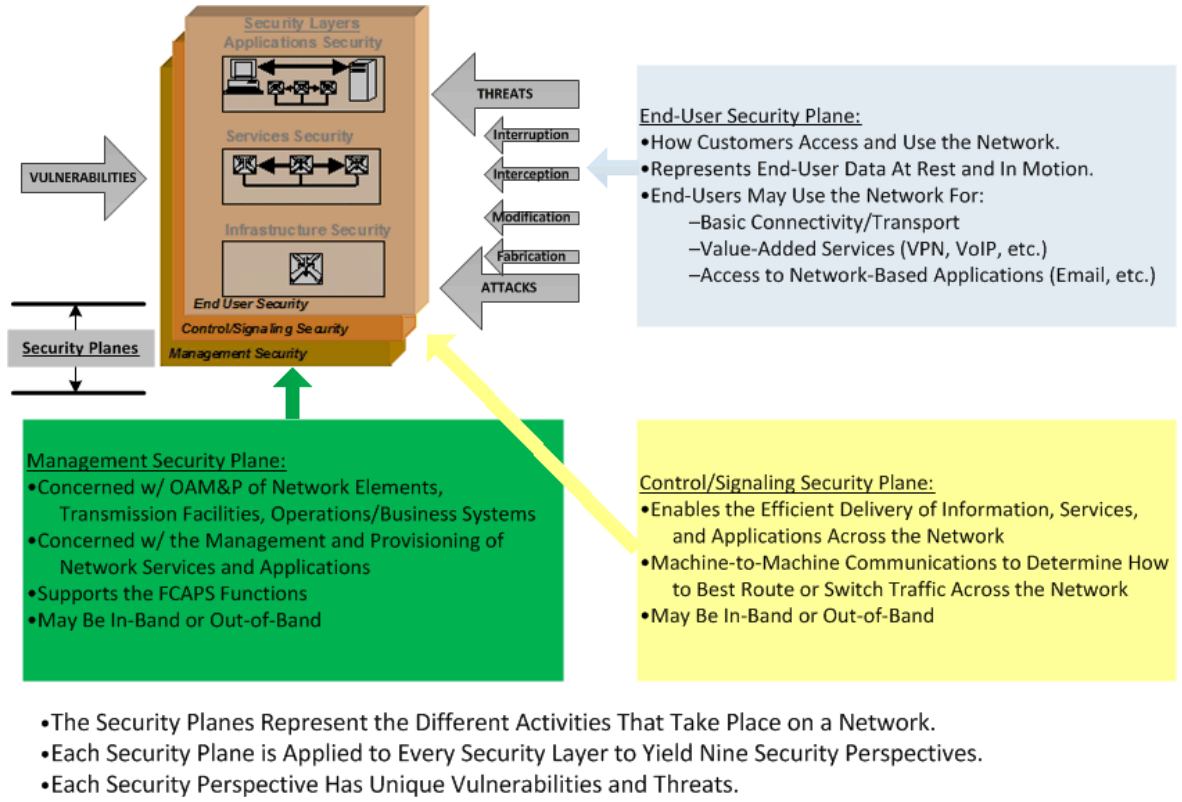


Figure D.1.1.2-1: Security Planes

The concept of Security Planes is used for ensuring that essential network activities are protected independently (e.g. compromise of security at the End-user Security Plane does not affect functions associated with the Management Security Plane). Moreover, the concept of Security Planes allows to identify potential network vulnerabilities that may occur when distinct network activities depend on the same security measures for protection

D.1.2.3 Combination of layers and planes

In X.805, each Security Plane is applied to every Security Layer. This leads to nine security perspectives (3x3).

Table D.1.2.3-1 : Security Perspectives

	Infrastructure Layer	Service Layer	Application Layer
Management Security Plane	Security Perspective 1	Security Perspective 4	Security Perspective 7
Control Security Plane	Security Perspective 2	Security Perspective 5	Security Perspective 8
End-User Security Plane	Security Perspective 3	Security Perspective 6	Security Perspective 9

This approach permits to provide a modular, systematic and organized way for performing network security assessments and planning.

Each security perspective has unique threat and vulnerabilities and in every of these perspectives, security objectives can be derived.

Below is an example referring to the Security Perspective 3 reported in Table D.1.2.3-1.

Table D.1.2.3-2: Example of security objectives for Infrastructure Layer / User Data Plane in the 8 security dimensions of X.805

Security Dimension	Security Objectives
Access Control	Ensure that only authorised personnel or devices are allowed access to end-user data that is transiting a network element or communications link or is resident in an offline storage device.
Authentication	Verify the identity of the person or device attempting to access end-user data that is transiting a network element of communication link or is resident in an offline storage device. Authentication techniques may be required as part of Access Control.
Non-repudiation	Provide a record identifying each individual or device that accessed end-user data that is transiting a network element or communication link, or is resident in offline devices and that the action was performed. The record is to be used as proof of access to end-user data.
Data Confidentiality	Protect end-user data that is transiting a network element or communication link, or is resident in an offline storage device against unauthorised access or viewing. Techniques used to address access control may contribute to provide data confidentiality for end-user data.
Communication Security	Ensure that end-user data that is transiting a network element or communication link is not diverted or intercepted as it flows between the end point (without an authorised access).
Data Integrity	Protect end-user data that is transiting a network element or communication link or is resident in offline storage devices against unauthorised modification, deletion, creation and reputation.
Availability	Ensure that access to end-user data resident in offline storage devices by authorised personnel and devices cannot be denied.
Privacy	Ensure that network elements do not provide information pertaining to the end-user network activities (e.g. Users geographic location, websites visited, content etc.) to unauthorised personnel

D.1.3 Complete picture and conclusions for this approach

In the following figure the complete ITU-T X.805 security architecture is shown:

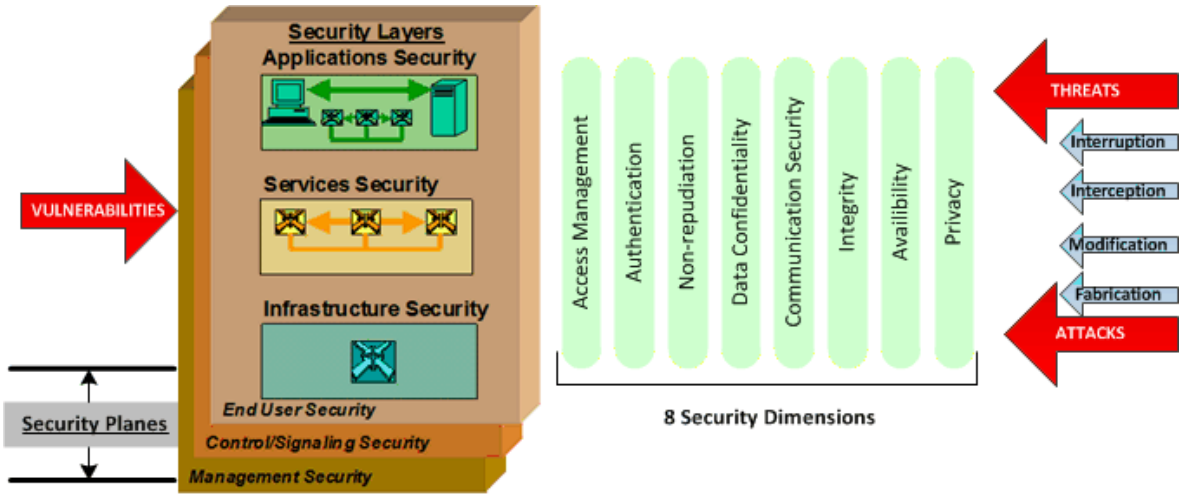


Figure D.1.3-1: ITU-T X.805 security architecture

This approach is able to provide a comprehensive, end-to-end network view of security. It can be applied to any network technology (e.g. wireless, wireline, optical networks) and to a several networks (e.g. service providers' networks, data centers' networks, government's networks and so on). Finally it is aligned with other security ITU-T Recommendations and ISO standards.

Even if this approach is very complete and ensures coverage of all cross-layer interactions in the definition of threats, the final concrete usage of it might be heavy if applied again for all network product classes.

Editor's note: Whether the threat analysis could be done per SAS modules instead of per network product class in order to ensure modularity and reuse of what is common to all network product classes is FFS.

Editor's note: To which extend X.805 could concretely fit to this approach per SAS module is FFS.

D.2 Threats classifications by looking at the sources of attacks

D.2.1 Overview

Another way of classifying the threats is to look at the different interfaces and sources of attacks. The figure below present attacks on an LTE network categorized by attacks happened in different domain.

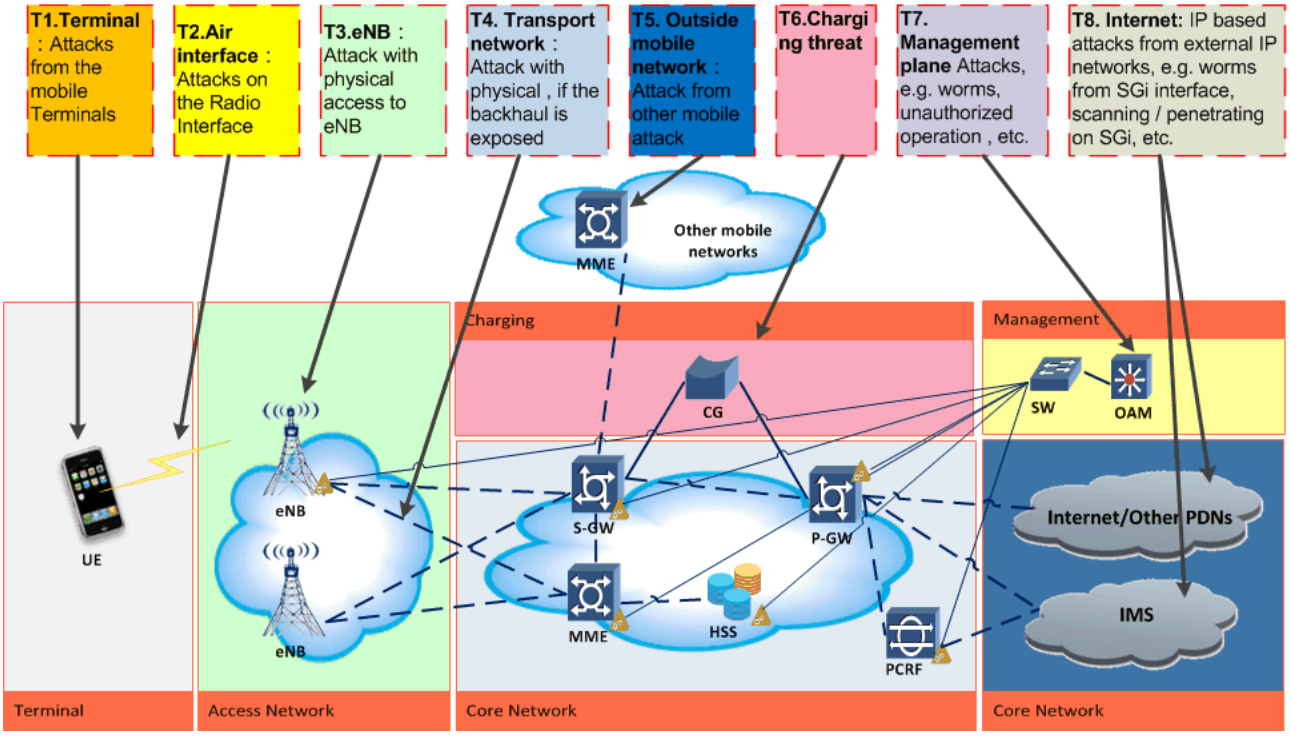


Figure D.2.1-1: threats classification example by attack sources

NOTE 1: The figure is not intended to cover all attack cases and could be refined.

The figure looks at the threat from a different angle but some correspondences with ITU-T X.805 can be found. As for the security planes for example:

- End–user Security Plane <->T1.
- Management Security Plane <-> T6, T7, T8
- Control/Signalling Security planes <-> T1, T2, T3, T4, T5

NOTE 2: This mapping is just an example not exhaustive.

The various 8 (T1-T8) threats classifications are intended to deal with the threats for the different parts of the network as examples. Of course, maybe it needs further analysis to see if it has covered all of the threats classes.

- T1 summarizes the threats coming from the terminal, e.g., a malicious or compromised UE can be used to initiate DoS attack to eNB/MME, detect the topology of core network, or any other type of attacks.
- T2 summarizes the threats related to the air interface and communication path. Attacker can launch attacks on air interface such as, for example, eavesdropping, modifying and forging the signalling or user data on this interface.
- T3 summarizes the threats raised by a physical access to a RAN network device. For example this type of attack can target eNB network product class a console interface access violation.

- T4 summarizes the threats identified for the transport network. If the backhaul link is exposed without physical protection, an attacker who can access the backhaul link could eavesdrop or modify the messages transported in the link.

- T5 summarizes the threats coming from other external interconnected networks (e.g. GRX/IPX, other PLMNs and so on) and targeting for example MME/S-GW/P-GW. For example, an operator A, in order to provide roaming service to end users, has to establish connections with external mobile operator networks. So the operator A's MME/S-GW/P-GW has to be accessed by external mobile operator's network products.
  If a network product in an external mobile operator network is compromised, it can be used to attack to the operator A's network.

- T6 refers to threat coming from the internal networks, mostly for the charging. Insider attacker like disgruntled employee from operator could also try to attack charging system through MME/S-GW/P-GW.

- T7 summarizes the threats for the OAM side similar to T6. Disgruntled employee will try to attack MME/S-GW/P-GW through management plane by remote management application or by physical interface.

- T8 summarizes the threats coming from Internet or another connected packet data network (PDN), e.g. a corporate/partner IP network. The attacks coming from these PDNs could violate the border security protections (e.g. FW) to inject virus, worms, Trojan-horses into core network or make some other types of attacks.

Annex E:
Vendor network product development and network product lifecycle management process assurance requirements

E.1 Example of requirements from CPA Build Standard

These requirements are taken from the CPA Build Standard [18] at Foundation Grade Evaluation Level with wording adaptation to fit in SECAM vocabulary. The "Test cases" are given for information in order to better describe the requirement and are short version of the "Assurance Activities" from the CPA Build Standard [18]. To have more details on the test case and approximate correspondence to the equivalent CC components, the reader is invited to read [18]. Annex E.2 will provide a mapping of these 13 requirements into the 4 blocks of requirements from 5.2.4.1. Below, the requirements that would map to the "Flaw remediation" bloc are given as examples.

2. Updates that fix security flaws must be actively advertised to supported customers and categorised according to the severity of the flaw.

   - Test case: The Accreditor must examine the Product Vendor's processes for informing customers of security issues discovered in their product, and ensure that these will ensure an effective and timely distribution of information.

5. The Vendor must use defined processes for flaw remediation, and show that Vendors are trained in these processes. The Vendor must also show that mechanisms are in place to ensure that this process cannot be bypassed by the Vendor.

   - Test case: The Accreditor must investigate the Vendor's flaw remediation processes, and ensure that they are applicable to any realistic problems

9. Flaw remediation is performed in practice.

   - Test case: The Accreditor must seek evidence that the Vendor's flaw remediation procedures are routinely followed in practice. The Vendor must also be able show to the Accreditor how a random sample of issues discovered (from minor to major) at all points in the product's lifecycle have been managed from discovery, through analysis, correction, testing and ultimate resolution.

12. Externally reported flaws in the Vendor's products must be handled appropriately

    - Test case: The Accreditor must seek evidence that the Vendor has a process for receiving externally discovered flaws that are reported. This process must be routinely followed in practice.

E.2 Mapping of the example requirements to Vendor NP Development and NP lifecycle management Assurance blocks

- Version and configuration management
  - Requirements {1;3;4;7}
- Flaw remediation
  - Requirements {2;5;9;12;}
- Process to ensure code quality
  - Requirements {8;10;11;13}
- Vendors development sites protection
  - Requirements {6}

Annex F:
Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
2012-11					Initial version after SA3#69 meeting	-	0.1.0
2013-01					Version after SA3#70 meeting before email approval process of the remaining contributions	0.1.0	0.2.0
2013-02					Editorial improvements	0.2.0	0.2.1
2013-02					Version after SA3#70 email approval process	0.2.1	0.3.0
2013-04					Version after SA3#71 meeting	0.3.0	0.4.0
2013-04					Editorial changes: bitmap pictures converted to editable ones	0.4.0	0.4.1
2013-06	SA#60	SP-130247			Presentation in SA Plenary for information	0.4.1	1.0.0
2013-07					Version after SA3#72 before approval of the remaining contributions	1.0.0	1.1.0
2013-08					MCC clean-up	1.1.0	1.1.1
2013-09					Version after SA3#72 email approval process	1.1.1	1.2.0
2013-09					Editorial improvements after second email approval	1.2.0	1.2.1