Network Equipment Security Assurance Scheme – Vendor Development and Product Lifecycle Requirements and Accreditation Process

Version v0.21

June 2016

Security Classification: Non-confidential

Copyright Notice

Disclaimer

Antitrust Notice

Table of Contents

1 Introduction

This document is part of the GSMA Network Equipment Security Assurance Scheme (NESAS), of which there is an overview available in FS.13 – NESAS Overview [1].

This document defines requirements for a vendor's development and product lifecycle processes. It also describes the accreditation process.

1.1 Scope

The scope of the document has been restricted only to matters pertaining to the Vendor Development and Product Lifecycle Accreditation Requirements and Process.

Consistency of the accreditation requirements has been achieved by defining:

- Vendor Development and Product Lifecycle
- Objectives to be achieved
- Assets to be protected
- Risk and threats against the objectives
- Accreditation requirements.

The number of requirements is kept relatively small (an order of magnitude of 10) to keep evaluation costs reasonable and to focus on critical controls.[1] It is taken into account that the CPA build standard integrates elements which will be explicitly covered by requirements in SCASes.

1.2 Document Maintenance

This standard has been created and developed under the supervision of GSMA's Security Assurance Group comprised of representatives from mobile telecom network operators and infrastructure suppliers.

The GSM Association is responsible for maintaining this security standard and for facilitating a review, involving all relevant stakeholders, which will take place every 12 months during the life of the scheme.

1.3 Applicability and use of the Vendor Development Process and Lifecycle Accreditation

3GPP TR 33.916 [3] describes the applicability and use of the accreditation of vendor network product development and network product lifecycle management as follows in section 6.2:

> Editor's note: Before the final document deliverable is created, above reference needs to be verified, and if required updated.
>
> 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 NESAS Accreditation Board.

[1] Compare Note 3 in TR 33.916 [3], section 6.2. The CESG's CPA build standard [4] is seen as inspiration for the abstraction level, amount, and content of the requirements.

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. 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 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.

2 Definitions

2.1 Common Abbreviations

Term	Description
3GPP	The 3rd Generation Partnership Project
CESG	Pseudo acronym; The UK National Technical Authority for information assurance.
CPA	Commercial Product Assurance
FASG	Fraud and Security Group
SCAS	Security Assurance Specification
SHA-512	Secure Hash Algorithm-512
SECAM	Security Assurance Methodology
SECAG	Security Assurance Group
NESAS	Network Element Security Assurance Scheme
NIST	National Institute of Standards and Technology
TR	3GPP Technical Report
TS	3GPP Technical Standard

2.2 Glossary

Term	Description
NESAS Accreditation Board	The body overseeing NESAS, run by the GSMA. It is responsible for Vendor Development and Product Lifecycle accreditation, and conflict resolution.
Accreditation Certificate	Document stating the successful outcome of an audit including a hash over the Audit Report.
Appointed GSMA Staff	Operational entity within the GSMA, organizing audits. This entity consists exclusively of GSMA staff.
Audit Company	Optional entity. Organization contracted by the GSMA to provide the Audit Team.
Audit Guidelines	Document giving guidance to the Audit Team and Auditee on how to interpret the requirements.
Audit Report	Deliverable of the work executed by an Audit Team.
Auditee	Entity being subject to an audit.
Commercially Relevant Lifetime	Commercially relevant is the time during which the Network Product it operated in a production network and maintenance by the supplier is required by means of commercial agreements or regulatory stipulations.
Dispute Resolution Committee	The impartial interpreter of NESAS processes and documentation that is required to adjudicate on disputes that may arise between two or more parties.
Documentation	There are two different types of documentation. The term can either refer to documents that pertain to the product or to the Vendor Development and

Term	Description
	Product Lifecycle Accreditation Requirements and Process.
Firmware	Binaries and associated data supporting low-level hardware functionality installed on non-volatile memory like ROM and EPROM usually not mountable to a running operating system's file system. Firmware is a specific type of Software, therefore in this document the term "Software" includes Firmware.
GSMA Audit Report	Document summarizing the results of the audit conducted at the equipment Vendor by the GSMA Audit Team
GSMA Audit Team	Audit personnel used by GSMA to conduct equipment Vendor audits
NESAS Accreditation Board	Responsible for developing requirements on vendor network product development, network product lifecycle management process, and NESAS accreditation of vendors and NESAS security test laboratories
NESAS Dispute Resolution Process	The process used by the NESAS DRC to reach a ruling/decision.
NESAS Dispute Resolution Committee (DRC)	The impartial interpreter of NESAS processes and documentation that is required to adjudicate on disputes that may arise between two or more Parties.
Network Product	Network equipment produced and sold to network operators by an equipment Vendor
Network Product Class	In the context of SECAM, the class of products that all implement a common set of 3GPP defined functionalities.
Network Product Development Lifecycle	The stages through which products journey throughout their development including planning, design, implementation, testing, release, production and delivery.
Network Product Lifecycle	The stages through which developed products journey to end of life including maintenance and update releases during their lifetime.
Release	Version of a Network Product being made available for deployment. The first Release of a Network Product can be assumed to be a new Network Product.
Software	Binaries and associated data forming the basis of a Network Product's operating system and functionality. Software is commonly stored on hard disks or flash memory mass storage devices. In this document, the term "Software" includes "Firmware".
Vulnerability	In SP 800-30 [5], NIST defines a vulnerability as "A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy."

2.3 References

Ref	Title
[1]	FS.13 -– Network Equipment Security Assurance Scheme – Overview
[2]	"Key words for use in RFCs to Indicate Requirement Levels", S. Bradner, March 1997. http://www.ietf.org/rfc/rfc2119.txt
[3]	3GPP TR 33.916, "Security assurance scheme for 3GPP network products for 3GPP

Ref	Title
	network product classes". http://www.3gpp.org/DynaReport/33916.htm
[4]	"CPA Build standard", contains the CESG's requirements for a product developer's security engineering approach. http://www.cesg.gov.uk/Publications/Documents/the_cpa_build_standard.pdf
[5]	NIST SP 800-30 Rev. 1, "Guide for Conducting Risk Assessments" September 2012. http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf
[6]	NIST FIPS PUB 180-4 "Secure Hash Standard (SHS)", August 2015. http://dx.doi.org/10.6028/NIST.FIPS.180-4

2.4 Conventions

The key words "must", "must not", "required", "shall", "shall not", "should", "should not", recommended", "may", and "optional" in this document are to be interpreted as described in RFC2119 [2]."

3 Definition of Vendor Development and Product Lifecycle

3.1 Introduction

Protection of relevant assets, as defined in section 4, needs to be in place during the entire Commercially Relevant Lifetime of a Product.

Within NESAS, the Vendor Development and Product Lifecycle covers all aspects potentially impacting a Network Product's Commercially Relevant Lifetime, relating to it being planned, implemented, delivered, updated, and eventually ramped down. The accreditation requirements defined in section 7, intended to mitigate the relevant threats defined in section 5, are to be implemented within the Vendor Development and Product Lifecycle defined within this section.

3.2 Development Lifecycle

The Development Lifecycle can be broken down into a number of high-level phases which are executed sequentially. The high-level phases are listed in **Fehler! Verweisquelle konnte nicht gefunden werden.**.

#	Title	Description
1.	Active Development	In this phase, new features are commonly added in new releases.
2.	Maintenance	The phase in which features are not actively added to the product but commercial agreements or relevant regulatory requirements exist to maintain the products in operation by providing updates to correct vulnerabilities and other bugs.
3.	Ramp Down	In this phase actions are taken to end a product's lifetime and cease any maintenance. This phase commonly marks the end of a product's commercially relevant lifetime.

Table 1Development Lifecycle; High-Level phases

Usually, the low-level phases within the "Active Development" high-level phase are pretty similar to the ones in the "Maintenance" high-level phase. They are executed in a cyclic fashion, starting again from the beginning once finished. The low-level phases are listed in **Fehler! Verweisquelle konnte nicht gefunden werden.**.

#	Title	Description
1.	Planning	In case of a completely new Network Product, the requirements for the first Release are planned. In case of a new version for an existing product, the requirements for the changes to be introduced by the next release are planned based on updated functional requirements as well as bug and vulnerability reports received against prior versions, if applicable.
2.	Design	The implementation of the planned requirements for the Release is planned in detail.
3.	Implementation	The planned requirements are implemented as per the design.
4.	Testing and Verification	The fulfilment of the requirements by the implementation is

#	Title	Description
		verified. If the verification fails, the relevant requirement usually goes back to the “Implementation” phase. This phase also contains the security related testing and verification activities.
5.	Release	The decision to release a given revision of a tested and verified implementation.
6.	Manufacturing	In this phase, the development Release is converted into a deliverable product. In case of pure software delivery, this is the delivery of the Release to the provisioning process.
7.	Delivery	The delivery of the manufactured Network Product.

Table 2 Development Lifecycle; Low-level Phases

3.3 Product Lifecycle

The Product Lifecycle in the NESAS context concentrates on updates a Network Product receives during its lifetime. It can be broken down into a number of phases, listed in **Fehler! Verweisquelle konnte nicht gefunden werden.**.

#	Title	Description
1.	First Commercial Introduction	The Network Product starts its commercial lifetime by means of a first Release to be accepted for usage in life commercial networks. Before that, earlier Releases may have been tested in test environments.
2.	Update	The Network Product is updated by means of either a minor or a major Release. This phase usually is a cycle of such Releases.
2.1.	Minor Release	A minor Release fixes Vulnerabilities and other bugs found in earlier versions. It commonly introduces not more than minor feature enhancements and architectural changes.
2.2.	Major Release	A major Release fixes Vulnerabilities and other bugs found in earlier versions. It may introduce major feature enhancements and architectural changes.
3.	End Of Life	No updates for the Network Product are supplied anymore. As this phase occurs after contractual and regulatory requirements to maintain the Network Product have ceased, this commonly marks the end of a Network Product’s Commercially Relevant Lifetime.

Table 3 Product Lifecycle

4 Assets

4.1 Introduction

The ultimate goal of security related elements in the Vendor Development and Product Lifecycle is to ensure that the interests of the Operator are protected. Usually, the main interest of the Operator is the flawless operation of its network. This section defines, discusses and prioritizes those security related assets which could have a negative impact on an operator's network if they are harmed.

Assets in the scope of this document are the Network Product and its constituent parts that exist during the Vendor Development Lifecycle. The assets need to be protected from threats that could lead to Vulnerabilities in the Network Product during its lifecycle. Protection of relevant assets needs to be in place during the whole Commercially Relevant Lifetime of a Network Product.

Security Objectives will be derived from the assets and identified relevant threats and defined in section 6.

The identified relevant assets are laid out in the following sections.

4.2 Source Code (SRC)

Source code is used to create a Network Product's binary Software. Here, the term "source code" also includes scripts which are not necessarily compiled to binary but are included as-is in the Network Product's Software.

Common types of source code include those:

- Created by the vendor dedicated for use in one or more particular Network Products of the vendor **[SRC_VND]**
- Created by a subcontracting 3rd party on behalf of the vendor dedicated for use in one or more particular Network Products of the vendor **[SRC_SUB]**
- Created as general software element (e.g. libraries) by a 3rd party supplier and provided to the vendor as binary **[SRC_TRB]**
- Created as general software element (e.g. libraries) by a 3rd party supplier and provided to the vendor as source **[SRC_TRS]**
- Created by a 3rd party as free and open source without support **[SRC_FOS]**

4.3 Software Packages (SPK)

Software packages are commonly created out of source code (SRC) during the Active Development and Maintenance phase through a build process. They are then subjected to Testing and Verification as well as Release decisions – and potentially used for Manufacturing.

One Network Product contains a combination of multiple Software Packages after manufacturing.

Common types of Software Packages include those:

- Created by the vendor **[SPK_VND]**

- Created by a subcontracting 3rd party on behalf of the vendor **[SPK_SUB]**
- Created by a 3rd party supplier **[SPK_TRD]**

4.4 Finished Products (FIN)

Finished Products typically are:

- Software images for installation on Network Products **[FIN_SWR]**, typically compiled out of one or more Software Packages (SPK)
- Hardware integrating the whole Network Product **[FIN_HWR]**, typically already including a certain release of FIN_SWR after the production process.

4.5 Security Documentation (DOC)

Security Documentation is used to guide product design and develop source code and is a deliverable during the product design and development process.

A common type of Security Document includes that created by the vendor during product design and development process, e.g. schematics or architecture design documents. **[DOC_DES]**

4.6 Operated Products (OPP)

Operated Products are those that are in active use by an operator. These are FIN_HWR that can be, and already might have been, updated with new FIN_SWR after they have been first delivered by the vendor.

- Network Products operated in life networks **[OPP_LFE]**

4.7 Product Development Support System (SUP)

Support Systems are used to manage activities, documentation, and source code in the product development process, throughout the entire lifecycle.

Common types of Support System:

- Product build environment, including compilation environment and tools used in the product compilation process. E.g. operating system, compile scripts, build tools. **[SUP_BUI]**

5 Threats and their Risks

5.1 Introduction

This section defines threats and analyses the associated risks.

A risk analysis is done to identify the main threats against the assets. The list is not intended to be exhaustive but shall focus on identifying those threats that introduce the highest risks. The referenced assets affected by the threats are always those which are directly affected if the threat materializes. The impact on these assets could potentially propagate through other assets, in the end impacting the flawless operation of an operator's network and other operations.

The threats are listed in sections 5.3 (critical), 5.4 (major), 5.5 (intermediate), and 5.6 (minor), independently of the lifecycle step concerned.

5.2 Risk analysis

The magnitude of a risk originated by a threat is calculated as the product between the likelihood of a threat occurring and the severity of the consequences (impact) for the operator using the product.

$$Risk\ Magnitude = Likelihood \times Impact$$

Equation 1 Calculation of Risk Magnitude

The likelihood, in this document, represents a qualitative parameter expressed in terms of one of four levels provided in **Fehler! Verweisquelle konnte nicht gefunden werden.**.

These levels have been identified counting the likelihood of a threat becoming a reality and possibly affecting an operator negatively.

In order to quantify the risk magnitude, each likelihood level has been mapped to a numeric value (score).

Score	Likelihood Level	Definition
4	Very likely	Threat easily materializes even without attacker involvement. Possibility of detection is minimal.
3	Likely	Materialization of threat is possible. An attacker has high incentive for active involvement even with high cost. Possibility of detection is not very high.
2	Possible	Skilled and motivated attacker can trigger the materialization of the threat with reasonable cost and/or risk of getting caught exists.
1	Not likely	Materialization of the threat on its own is very unlikely. Triggering it would be unreasonably expensive or otherwise not interesting for an attacker and/or risk of getting caught is high.

Table 4 Likelihood

The impacts, in this document, represent a qualitative parameter expressed in terms of one of four levels**Fehler! Verweisquelle konnte nicht gefunden werden.**.

These levels have been identified considering how significant the impact is likely to be for an operator if the threat becomes a reality. As is done for threat likelihood, the impact levels are mapped to numeric values (score) used to quantify the magnitude of a risk.

Score	Impact Level	Definition
4	Disastrous	Regulatory violation & Service or Network outage & Significant Loss of Revenue
3	Damaging	Regulatory violation, Service or Network outage, Significant Loss of Revenue
2	Harmful	Significant performance degradation. Fault impacting significant part of network
1	Annoying	Localised Fault, Performance degradation tolerable, minimal loss of revenue

Table 5 Impact

As described in Equation 1, the Risk Magnitude is a cross product between the vector of the likelihood levels/scores and the vector of the impact levels/scores. The result is the matrix shown in **Fehler! Verweisquelle konnte nicht gefunden werden.**.

Very likely (4)	Intermediate (4)	Major (8)	Critical (12)	Critical (16)
Likely (3)	Minor (3)	Intermediate (6)	Major (9)	Critical (12)
Possible (2)	Minor (2)	Intermediate (4)	Intermediate (6)	Major (8)
Not likely (1)	Minor (1)	Minor (2)	Minor (3)	Intermediate (4)
	Annoying (1)	**Harmful (2)**	**Damaging (3)**	**Disastrous (4)**

Table 6 Risk Magnitude Matrix

Finally, the obtained numeric values of the risk magnitude are mapped to four risk levels that express the risk severities: Critical, Major, Intermediate and Minor.

The risk level of an identified threat is always calculated with the assumed highest likelihood and the worst impact for an operator following best industry practices for securing its network. There is no differentiation considered for individual operators.

5.3 Critical Threats Descriptions

Editor's Note: The exercise of assigning probabilities and impact to threats as well as assigning threats to sections 5.2 through 5.5 needs to be done before final document release. This is not considered to be an absolute requirement for the pilot.

Critical risks must be mitigated through derived objectives when meaningfully possible, leading to requirements with a high return on investment.

Threat	Assets	Prob.	Impa.	Description
T_ROGUE_DEV	SRC_VND SRC_SUB	TBD	TBD	A rogue developer secretly introduces a Vulnerability into source code dedicated for use in the Network Product.
T_VULN_SRC_OWN	SRC_VND SRC_SUB	TBD	TBD	Source code dedicated for use in the Network Product leads to a Vulnerability.
T_VULN_SRC_OTHER	SRC_TRB SRC_TRS SRC_FOS	TBD	TBD	General source code by a third party leads to a Vulnerability.
T_POOR_DES	FIN_SWR FIN_HWR OPP_LFE	TBD	TBD	A design flaw of the Network Product leads to a Vulnerability. Lacking/insufficient security considerations in architecture or design of the product are the cause. Attackers can bypass or destroy the defence system due to inappropriate security design or design omission to launch attacks.
T_UNTRUSTED_SWR	OPP_LFE	TBD	TBD	A recipient of a Software image for installation on a network product receives a non-genuine Release, potentially including a Vulnerability.
T_VULN_SWR	OPP_LVE	TBD	TBD	A recipient of a Software image for installation on a network product receives an old version re-introducing old Vulnerabilities.
T_FIX_UNAWARE	OPP_LVE	TBD	TBD	An operator is not aware

Threat	Assets	Prob.	Impa.	Description
				of available Software updates for an operated Network Product. This extends the window of vulnerability in which defensive measures against a hostile environment are reduced.
T_VULN_UNAWARE	SPK_TRD FIN_SWR	TBD	TBD	A vendor does not become aware of Vulnerabilities caused by used 3rd party components.
T_VULN_NOHANDL	SPK_VND SPK_SUB FIN_SWR	TBD	TBD	Vulnerability found by vendors, operators, or other 3rd party, and made known to the vendor is not appropriately handled.
T_SENSITIVE_DOC_LEAK	DOC_DES	TBD	TBD	Security documents containing sensitive information about the Network Product are leaked. This could be utilized by malicious attackers to find out Vulnerabilities and launch related attacks.
T_BLDTOOL_TAMPER	SUP_BUI	TBD	TBD	A malicious attacker may damage the system by replacing relevant tools, revising the related parameters or implanting malicious programs through compilation environment.
T_WRONG_DOC	FIN_SWR FIN_HWR OPP_LFE	TBD	TBD	The customer documentation for the Network Product does not cover the actual functionality and properties of the Network Product.
T_NO_CONTACT	OPP_LFE	TBD	TBD	The customer vendor has no or not the right contact at the vendor organisation to address any security inquiries or

Threat	Assets	Prob.	Impa.	Description
				incidents.

Table 7 Critical Risk Threats Descriptions

5.4 Major Risk Threats Descriptions

Major risks must be mitigated where effective derived objectives, leading to requirements with a reasonably high return on investment, can be identified.

Threat	Assets	Prob.	Impa.	Description

Table 8 Major Risk Threats Descriptions

5.5 Intermediate Risk Threats Descriptions

Intermediate risks should be mitigated where effective derived objectives, leading to requirements with a high return on investment, can be identified.

Threat	Assets	Prob.	Impa.	Description

Table 9 Intermediate Risk Threats Descriptions

5.6 Minor Risk Threats Descriptions

Minor risks do not need to be mitigated.

Threat	Assets	Prob.	Impa.	Description

Table 10 Minor Risk Threats Descriptions

6 Security Objectives

6.1 Introduction

The accredited entity is responsible for ensuring that assets are protected from the risks to which they are exposed; as defined by the security objectives. It is this protection that provides assurance to the operators. All the objectives must be addressed but higher levels of assurance are needed depending on the asset classification and the return on investment for the actual security level of the network product.

The security objectives have been defined based on their effectiveness to mitigate the threats and to provide a return on investment.

Section 6.2 lists the Security Objectives for the Development Process and Product Lifecycle.

6.2 Security Objectives

Identifier	Objective	Threats	Description
O_CONTROL	All source code changes are controlled. It is possible to reconstruct the reason for code changes.	T_ROGUE_DEV	To lower the risk that Vulnerabilities are introduced on purpose.
O_VUL_INT	Software dedicated for a Network Product is free of vulnerabilities.	T_VULN_SRC_OWN	To lower the risk of accidental occurrence of Vulnerabilities.
O_VUL_PAT	Discovered Vulnerabilities are addressed appropriately and timely.	T_VULN_SRC_OWN T_VULN_SRC_OTHER T_VULN_NOHANDL	To reduce the window of opportunity originating from a known Vulnerability.
O_PROT_DOC	Sensitive documents do not leak.	T_SENSITIVE_DOC_LEAK	To protect sensitive information from becoming known to potential attackers.
O_PROT_BLDTOOL	Compilation and build environment is protected from tampering.	T_BLDTOOL_TAMPER	To lower the risk that replaced build tools or manipulated parameters introduce Vulnerabilities to the Network Product through the compilation environment.
O_VULN_AWARE	Newly found Vulnerabilities originating from	T_VULN_UNAWARE	To ensure that known Vulnerabilities can be mitigated for operated

Identifier	Objective	Threats	Description
	used 3rd party components are identified as early as possible.		Network Products within an appropriate time and don't go undetected although they may be publicly known.
O_GENUINE_SWR	Software integrity is verifiable by appropriate means before it is installed in a product.	T_UNTRUSTED_SWR	To prevent maliciously tampered Software loads being accidentally installed.
O_IDENT_SWR	Individual Software load versions are identifiable by appropriate means.	T_VULN_SWR	To prevent old versions of software from being accidentally installed in operated products and old Vulnerabilities being re-introduced in networks.
O_INFORM_FIX	Operators are informed of available security related fixes for the Network Product in a timely manner.	T_FIX_UNAWARE	To ensure that operators are made aware of available fixes and are able to apply them in order not to unnecessarily extend the window of vulnerability within their networks.
O_TRA_ANALYSE	Security is built into the design from the very beginning.	T_POOR_DES	Security-by-design ensures Vulnerabilities can be mitigated by a secure design of the product.
O_SEC_TEST	Testing demonstrates secure and robust implementation of the Network Product.	T_ROGUE_DEV T_POOR_DES	During testing of the product, security is tested in order to determine vulnerabilities, unexpected behaviour, unspecified behaviour and robustness against undefined input.
O_STAFF_EDU	Staff involved in design, engineering, development, implementation, and maintenance is sufficiently	T_VULN_SRC_OWN	Staff that is involved in creating the Network Product and its upgrades is educated and experienced in relevant network and IT security matters so that

Identifier	Objective	Threats	Description
	aware of IT/network security matters.		they can create a secure Network Product.
O_ACCURATE_DOC	An accurate and up-to-date customer documentation of the Network Product exists, which describes all details that affect the Network Product's security. The documentation matches the development state of the Network Product (HW, SW, functionality, configuration).	T_WRONG_DOC	The customer documentation related to security matters is accurate and describes the actual functionality and properties of the Network Product as it is delivered to operator customers.
O_SEC_POC	For all security inquiries the operator customer knows who to approach in the vendor organisation.	T_NO_CONTACT	There is a clear communication from the vendor to its operator customers to let operators know who to contact for any security inquiries or incidents.

Table 11 Security Objectives for the Development Process and the Product Lifecycle

7 Requirements

7.1 Introduction

In order to have sufficient confidence in the Vendor Development and Product Lifecycle certain requirements must be met. These requirements, which are outlined below, are considered as minimum requirements.

The requirements have been selected based on their effectiveness to fulfil the objectives and provide a return on investment. Each requirement fulfils one or more security objectives, while one or more requirements may exist to fulfil the same Security Objective.

The requirements of the Standard should be met by established processes/controls for which evidence of correct operation exists.

It is recognised that it is possible to use mechanisms or tools other than those described in this section if they achieve the same security objective.

7.2 Design

7.2.1 [REQ-01] Security by Design

The product shall implement security by design throughout the whole development lifecycle. Therefore, architecture and design decisions shall be made with security in mind. In the design phases, a threat analysis process for the product shall be undertaken to identify the potential threats and related mitigation measures. **[O_TRA_ANALYSE]**

7.3 Implementation

7.3.1 [REQ-02] Version Control System

During the entire commercially relevant lifetime of a product, the vendor shall utilize a version control system ensuring individual non-repudiation of source code commits. **[O_CONTROL]**

7.3.2 [REQ-03] Change Tracking

The vendor shall establish a documented procedure to ensure that all requirements and design changes, which may arise at any time during the product life cycle and which impact the Network Product (this includes source code dedicated for a product, open source and 3rd party software, documentation, requirement documents, and design documents), are managed and tracked in a systematic and timely manner appropriate to the life cycle stage. **[O_CONTROL]**

7.3.3 [REQ-04] Source Code Review

The vendor shall ensure that new and changed source code dedicated for a product (i.e. not “Off The Shelf” software) is appropriately reviewed in accordance with an appropriate coding standard. If feasible, the review should also be implemented by means of utilizing a Source Code Analysis Tool. This will help to reduce the risk of software issues which could cause Vulnerabilities in the Network Product**. [O_VUL_INT]**

7.3.4 [REQ-05] Software Security Testing

Software is to be tested from a security perspective. This testing shall identify and resolve issues potentially causing Vulnerabilities in the Network Product. Security testing consists of manual and automated tests with tool support, and investigative approaches. It is necessary to test the absence of dangerous/unwanted behaviour, as well as the robustness of the Network Product against undefined/unexpected input. Security testing is complementary to feature testing where only specified functionality is being tested. **[O_VUL_INT], [O_SEC_TEST]**

7.3.5 [REQ-06] Staff Education

Continuous education of staff involved in Network Product design, engineering, development, implementation, and maintenance shall be provided to ensure knowledge and awareness on security matters are maintained at a constantly high level. **[O_STAFF_EDU]**

7.4 Maintenance

7.4.1 [REQ-07] Vulnerability Remedy Process

The vendor shall establish a process to deal with Vulnerabilities found in or in relation to released Network Products. Vulnerabilities shall be dealt with appropriately and, if applicable, patches/software upgrades shall be distributed to all operators in order to honour existing maintenance contracts within an agreed schedule. **[O_VUL_PAT]**

7.4.2 [REQ-08] Vulnerability Remedy Independence

For ease of deployment, the vendor shall have the facility to provide patches/software upgrades that close security vulnerabilities separately from unrelated patches/software upgrades that modify functionality of the Network Product. **[O_VUL_PAT]**

7.4.3 [REQ-09] Information Security Management System

In the entire lifecycle, the vendor shall employ an information security management system to avoid sensitive information, such as e.g. descriptions of proprietary algorithms, being leaked. **[O_PROT_DOC]**

7.4.4 [REQ-10] Automated Build Tool

The vendor shall utilize an automated build tool to compile the source code and store the build logs. **[O_PROT_BLDTOOL]**

7.4.5 [REQ-11] Build Environment Control

All the data (including source code, building scripts, compilation tools, and compilation environment) of the compilation build environment shall come directly from a version control system. **[O_PROT_BLDTOOL]**

7.4.6 [REQ-12] Vulnerability Information Management

The vendor shall have reliable processes in place to ensure it can become aware of newly revealed potential Vulnerabilities in used 3rd party components and to evaluate whether they result in Vulnerabilities in the Network Product. **[O_VULN_AWARE]**

7.4.7 [REQ-13] Software Integrity Protection

The vendor shall establish and maintain methods to ensure that the delivery of products is carried out under controlled conditions. The operator shall be provided with appropriate means to identify whether a received software package is genuine. **[O_GENUINE_SWR]**

7.4.8 [REQ-14] Unique Software Release Identifier

All released software package versions shall bear a unique identifier. **[O_IDENT_SWR]**

7.4.9 [REQ-15] Security Fix Communication

A process shall ensure that information regarding available security related fixes is communicated to operators that have maintenance agreements in place at the time the fix is released. **[O_INFORM_FIX]**

7.4.10 [REQ-16] Documentation Accuracy

Customer documentation shall be up to date in all security related aspects and reflect the current functionality of the Network Product at the time when both the Network Product, or software upgrades of it, and the customer documentation are shipped to the customer. **[O_ACCURATE_DOC]**

7.4.11 [REQ-17] Security Point of Contact

The vendor shall provide a point of contact for security questions/issues and communicate this point of contact to its customer operators. This point of contact shall be able to find the right person/department inside the vendor organisation for security concerns raised by a customer. **[O_SEC_POC]**

7.5 Mapping of Requirements to Lifecycle Stages

	Development Lifecycle; High-Level phases			Development Lifecycle; Low-level Phases							Product Lifecycle			
	Active Development	Maintenance	Ramp Down	Planning	Design	Implementation	Testing and Verification	Release	Manufacturing	Delivery	First Commercial Introduction	Minor Release	Major Release	End Of Life
[REQ-01] Security by Design	✓				✓						✓	✓	✓	
[REQ-02] Version Control System	✓	✓				✓					✓	✓	✓	
[REQ-03] Change Tracking	✓	✓		✓	✓	✓					✓	✓	✓	
[REQ-04] Source Code Review	✓	✓				✓					✓	✓	✓	
[REQ-05] Software Security Testing	✓	✓					✓				✓	✓	✓	
[REQ-06] Staff Education	✓	✓												
[REQ-07] Vulnerability Remedy Process	✓	✓								✓				

	Development Lifecycle; High-Level phases			Development Lifecycle; Low-level Phases							Product Lifecycle			
	Active Development	Maintenance	Ramp Down	Planning	Design	Implementation	Testing and Verification	Release	Manufacturing	Delivery	First Commercial Introduction	Minor Release	Major Release	End Of Life
[REQ-08] Vulnerability Remedy Independence	✓	✓						✓				✓	✓	
[REQ-09] Information Security Management System	✓	✓												
[REQ-10] Automated Build Tool	✓	✓						✓			✓	✓	✓	
[REQ-11] Build Environment Control	✓	✓						✓			✓	✓	✓	
[REQ-12] Vulnerability Information Management	✓	✓												
[REQ-13] Software Integrity Protection	✓	✓						✓	✓	✓	✓	✓	✓	
[REQ-14] Unique Software Release Identifier	✓	✓						✓		✓	✓	✓	✓	
[REQ-15] Security Fix Communication	✓	✓										✓		
[REQ-16] Documentation Accuracy	✓	✓												
[REQ-17] Security Point of Contact	✓	✓												

Table 12 Application of Requirements in the Process

Editor's Note: The content of **Fehler! Verweisquelle konnte nicht gefunden werden.** needs to be updated before the first official release of the document after the Pilot.

8 Audit Guidelines and Evidence

8.1 Introduction

In regard to the Network Product development process and the lifecycle management requirements, section 7.2.1 of TR 33.916 [3] refers to two different categories of evidence.

- Evidence that the process is in fact accredited by the NESAS Accreditation Board must be available to the test laboratory.
  This is the Audit Report as defined in section 9.1.6, and the Audit Certificate as defined in section 9.1.7.

- Evidence within a self-evaluation report that the accredited process was in fact implemented. This report is provided by the vendor to the test laboratory.
  Section 8.3 specifies how it is defined and what this evidence is.

Although not explicitly defined in TR 33.916 [3], there is also the following type of evidence to consider, and explicitly distinguished from other evidence.

- Evidence that the NESAS development and lifecycle requirements are sufficiently addressed by a vendor's generic processes. This is evidence evaluated by the Audit Team.
  Section 8.2 explains how this evidence is defined by the Audit Guidelines document.

8.2 Audit Guidelines Document

The way vendors implement the requirements defined in section 7 in their product development and product lifecycles might vary from vendor to vendor, or even for different Network Products by the same vendor. Therefore, it is not feasible a priori to precisely specify the evidence an Auditor has to look for while verifying that the requirements are sufficiently fulfilled.

To ensure comparability between NESAS vendor accreditations, i.e. between different vendors, different Auditors, and over time, the Auditors will collaborate to create an Audit Guidelines document.

The Audit Guidelines document describes, for each requirement as defined in section 7, which evidence is considered sufficient for an Auditor to come to the conclusion that a process fulfils a requirement. It also contains information on which evidence is to be provided to testing laboratories that shall be deemed to be sufficient.

This Audit Guidelines document is owned, and its versions are controlled, by the NESAS Accreditation Board. Guidelines defined by Auditors are indicative only and are likely to evolve and possibly become more prescriptive throughout the lifetime of NESAS. Should any involved party see the need to challenge any decision of an Auditor or the manner in which it was made, based on the Audit Guidelines, it may refer the matter to the Dispute Resolution Committee. The subsequent decision by the Dispute Resolution Committee must be seen as definitive.

8.3 Evidence for Application of Accredited Process

A vendor needs to provide a self-evaluation report to the testing laboratory containing a rationale in free form, showing that the accredited security relevant part of the generic process was effectively applied during the development of the network product under evaluation.

The testing laboratory will review this self-evaluation report and evaluate whether the rationale provided by the vendor provides enough evidence that the network product development followed the accredited process.

The documentation provided by the Auditee to the Audit Team before the start of the audit, as defined in section 9.3.1 contains evidence the vendor considers to be sufficient for demonstrating to a testing laboratory that the requirements as defined in section 7 have been fulfilled in practice for a particular Network Product. This evidence might need to be refined after feedback from the Audit Team during the course of the audit.

Auditor's requirements in regard to evidence which needs to be provided to testing laboratories are also in scope of the Audit Guidelines document as discussed in section 8.2

The Audit Report, as defined in section 9.1.6 contains details of which evidence is deemed to be sufficient for each of the requirements defined in section 7.

As vendors' processes might allow for different options on how to implement a particular process, there can also be options for what constitutes the required evidence. Evidence requirements shall be defined as loosely as possible to allow flexibility while concentrating on the actual need for proper evidence. This is in order not to trigger any unnecessary re-accreditation if irrelevant and/or exchangeable details in the process change. Such details could be e.g. tools, names, file locations, etc.

It is not desired that creation of evidence becomes an unnecessary burden for the vendor. Therefore, creation of required evidence should not exceed the extra effort outside of commonly employed industry practices, or significant alteration of existing processes otherwise adequate to fulfil the requirements.

If there are cases where the Audit Team finds that, due to the nature of a requirement no meaningful evidence actually proving that a requirement is sufficiently fulfilled, could be created or evaluated with reasonable effort, the requirement shall not trigger the need for a vendor to create any evidence, or for the test lab to evaluate any. The Audit Company shall inform the NESAS Accreditation Board about the issue providing detailed information and recommendations. The NESAS Accreditation Board shall fix the requirement in the NESAS standard in order to avoid the same issue occurring again in the future.

Editor's note: Reasonable effort definition is FFS. An example of unreasonable effort would be if the test lab would need to evaluate each instance of an often recurring decision made by a developer, and also sampling would not provide the means for a meaningful conclusion that the actual intention of the requirement can be assured comprehensively. The paragraph needs to be reviewed after the pilot.

9 Accreditation Process

In this section the accreditation process is described.

Stakeholders in NESAS should be made aware that the procedure of auditing the vendor's development and lifecycle process is different to how schemes such as TL9000, ISO9001 & ISO27001 operate. For those latter schemes the auditors check both the processes and the implementation of the processes and in addition there are periodic surveillance audits by the auditor to ensure that the vendor continues to comply with the accredited process. For NESAS a vendor's process will be audited and accredited and then the accredited test labs ensure that the audited processes are implemented for products and their releases evaluated according to the scheme.

9.1 Set-Up

9.1.1 Accreditation Request

When a vendor (Auditee) wants its development and product lifecycle processes audited in order to become accredited, the GSMA is informed. On receipt of the request the Appointed GSMA Staff logs the details.

To ensure that the audit leading to the accreditation can be carried out in the requested timescales, the Auditee should give sufficient notice of the desired audit dates and **Fehler! Verweisquelle konnte nicht gefunden werden.**provide scheduling guidance for the audit.

Notice provided for requested dates	Scheduling target
3 months	within 4 weeks of requested date
2 months	within 6 weeks of requested date
1 month	within 8 weeks of requested date

Table 13 Audit Scheduling Guidance

It always remains the responsibility of the Auditee to ensure that certification is in place to meet the requirements of any specific contract, customer, or bid. The Auditees should schedule their audits accordingly.

9.1.2 Confirmation of audit date

After logging the request details, the information is sent to the Audit Team which then contacts the Auditee to agree audit dates.

9.1.3 Contract

The vendor seeking accreditation enters into a standard agreement with the GSMA. Before the audit, the Auditee pays the GSMA for the conduct of the audit. Then, the GSMA Audit Team carries out the audit.

9.1.4 Confidentiality

Ownership of all information communicated to the Audit Team or otherwise gathered by the Audit Team during the audit stays with the Auditee.

As part of the contract with the GSMA the Audit Company will have signed a related Non-Disclosure Agreement (NDA) and may have a separate agreement with the Auditee.

9.1.5 Language

The language used in the course of the audit is English.

9.1.6 Report

Throughout the audit the Audit Team summarises the results in a report which is structured as shown in Annex B:

- An identifier for the audit, unique within NESAS
- A reference to the NESAS release under which the audit was conducted
- Audit summary and overall assessment
  (including recommendation to award or withhold accreditation,)
- Actions required
- Auditors' comments
- Details for each requirement (from section 7) which kind of evidence is to be considered as sufficient by a testing laboratory.

9.1.7 Accreditation Certificate

Awarding the Accreditation leads to the creation of an Accreditation Certificate by the appointed GSMA staff. This document is based on a template managed by the NESAS Accreditation Board and contains the following information:

- Vendor name
- Statement regarding the successful outcome of the audit.
- An identifier for the audit, unique within NESAS
- A reference to the applicable NESAS release
- A hexadecimal representation of the SHA-512 hash over the relevant final Audit Report document (defined in 9.1.6)

9.1.8 Validity

An awarded accreditation applies to the NESAS release applicable at the time of accreditation, and to the audited processes in place.

However in order to ensure accreditation remains current vendors will need to get their accreditation renewed, if one or more of the following applies:

- Their development and lifecycle process in scope of NESAS changes.
- A new NESAS release is issued, and the vendor wants to comply with that.

Note: There is no periodic reaccreditation. Customer or market requests will ensure that vendors initiate the re-accreditation of their development and product lifecycle process in order to demonstrate that their processes are aligned with the latest NESAS release.

9.1.9 Timeline

It is in the interests of all involved parties to keep the overall time for the audit as short as possible. This allows the Auditee to get the accreditation within a short timeframe and it allows the Audit Team to focus on the Auditee without delays and interruptions.

The entire audit, as outlined in section 9.3, shall be completed within a time frame of at most three months.

The Auditee must ensure that all required documents, information, and on-site visits can be provided accordingly. The Audit Team shall ensure it has have sufficient time within the necessary timeframe to perform the audit.

This timeline reflects the maximum lead time and not the actual labour time. The timeline already includes periods where one of the involved entities prepares for the next step and the other entity is inactive.

9.2 Audit Preparation

After audit dates have been agreed, the Audit Team and Auditee will liaise to agree arrangements for the audit and prepare for parts of the audit process as needed.

To avoid misunderstandings on which input needs to be delivered by the Auditee, the exact versions of the NESAS standard documents (requirements, guidance, etc.) applicable for the audit shall be explicitly agreed between all parties.

The Audit Team and Auditee will mutually agree on suitable technical means to validate the authenticity of submitted information and data encryption. For email communication the use of S/MIME with personal certificates is recommended for all parties.

Editor's Note: Preferences of the selected 3rd party auditors for technical means for authentication and encryption needs to be taken into account.

9.2.1 Audit Scope

The scope of the audit should be clearly stated and agreed between the Audit Team and Auditee to ensure that there is a clear understanding and expectation for all stakeholders. The audit scope should be agreed as early as possible in the audit preparation phase. The scope should include:

- the exact release of the NESAS documents applicable for the audit,
- the entities that will be involved in the audit (audit team, auditee and potentially any 3rd parties such as contractors that are employed by the auditee),
- the processes that will be reviewed during the audit,
- the location that will be included in the audit,
- the business groups/organisations that will be included in the audit.

Note: Details of the items listed above will be provided in the Audit guidelines document

9.2.2 Provisional agenda

A provisional agenda will be agreed at least one week before the audit. A sample agenda is included in Annex A. The sample agenda includes guidance for Auditees on information that should be prepared and submitted for each element of the audit.

Changes to the agenda may need to be made during the audit itself. Changes will be mutually agreed between the Audit Team and the Auditee.

9.3 Audit Proceedings

The Audit proceeds in order of the subsections given in this section.

9.3.1 Presentation and Documentation for the Audit Team

Before the start of the Audit, the Auditee provides the Audit Team with written documentation regarding its processes along with a reasoning of how it believes it complies with the requirements laid out in section 7.

At the start of the Audit, the Auditee and the Audit Team meet virtually or in person. During this meeting, the Auditee provides an overview of the information submitted. The Audit Team may use the opportunity to indicate if and where further clarification might be needed. Additional documentation should be submitted by the Auditee within an agreed timeframe.

9.3.2 Documentation review by the Audit Team – First Round

The Audit Team evaluates that the processes described in the submitted documentation are sufficient to fulfil the requirements as laid out in section 7. This is done according to the timeframe as given in the agreed agenda.

If applicable during the progress of the first round of document audit, the Audit Team may indicate to the Auditee which documentation is still missing and which requirements are not fulfilled by the information provided. The Auditee may communicate the missing information to the Audit Team.

9.3.3 Intermediate Audit Result Meeting

An intermediate audit result meeting is held after the Audit Team has evaluated all initially provided documentation, and supplementary information that may have been provided during the first round of the audit.

In this meeting, the Audit Team informs the Auditee which requirements may not be fulfilled according to the information it has available.

The findings in the intermediate version of the audit report will classify issues in terms of major or minor issues, or observations. Observations (positive or negative in nature) are merely for information.

It is mutually agreed within which timeframe the missing or modified documentation is handed over from the Auditee to the Audit Team. If requested by the Auditee, this timeframe must be at least four weeks (28 days) and not more than 8 weeks (56 days).

9.3.4 Documentation review by the Audit Team – Second Round

The Audit Team evaluates whether the full documentation provided by the Auditee fulfils the requirements as laid out in section 7. This is done according to the timeframe as given in the agreed agenda.

If applicable during the progress of the second round of document audit, the Audit Team may indicate to the Auditee which documentation is still missing and which requirements are not fulfilled by the information provided.

9.3.5 On-Site Audit

Note: The On-Site Audit described in this section applies for the generic accreditation and is not intended to be Network Product specific.

After the documentation has been reviewed and considered complete by the Audit Team, the audit continues on-site at the Auditee's premises. During the on-site audit, the Audit Team evaluates:

- If the processes that are documented are actively applied in the day-to-day business of the Auditee;
- If the Auditee has the staff, skills, equipment, working practices and resources to follow the processes defined in the documentation;
- If the staff is sufficiently trained on the processes and if the staff understands them.

During the on-site audit, the Auditee provides evidence to the Audit Team that the engineering and production departments of the Auditee effectively apply their processes as defined in the provided documents.

The on-site audit should last one working day and shall not exceed two working days. The Auditee shall provide information on which employees are within the scope of the accreditation and shall ensure that individuals selected by the Audit Team will be available for interview by the Audit Team.

It is at the discretion of the Audit Team how to conduct the on-site audit. It is recommended to the Audit Team to witness day-to-day product development activities and product maintenance activities, including interviews with architects, developers, engineers and other personnel as needed. The Audit Team should limit its activities to samples. It is not intended to audit the processes to their full extent.

9.3.6 Presentation of the Results

At the end of the audit, the Audit Team presents its findings to the Auditee. The Audit Team also creates the Audit Report that contains all the results and reasoning. This report is structured as defined in section 9.1.6.

The Audit Team reaches agreement with the Auditee that the draft Audit Report reflects the observations and results of the audit. Following agreement on the Audit Report, the Audit Team provides the Auditee and the appointed GSMA staff with the final Audit Report. T\he preferred file format is PDF.

9.4 Accreditation

On receipt of an Audit Report recommending accreditation, the appointed GSMA staff, in the absence of any request or instruction to the contrary from the Auditee, will forward the Audit Report to the NESAS Accreditation Board. The NESAS Accreditation Board makes the decision whether or not to award accreditation. If the NESAS Accreditation Board awards accreditation, an Accreditation Certificate, as defined in Section 9.1.7, is issued and sent to the Auditee. If the Auditee does not object, a copy is published on the public GSMA Web site.

Annex A Sample Audit Agenda

Editor's Note: The content of this sample agenda as referenced from section 9.2.1 will be developed by SECAG in cooperation with the selected Audit Companies during the pilot phase.

Annex B Audit Report Structure

Editor's Note: The content of this section needs to be updated and finalized in cooperation with selected audit companies

B.1 First Page:

- Headline: GSM Association NESAS Audit Report

- Audit identifier
- A reference to applicable NESAS release
- Name of the *Auditee*
- Date of the audit

- *Audit Team* participants

B.2 Following Pages:

- Audit summary and overall assessment
- Recommendation to award or withhold accreditation
- Actions required (what to do and maybe also how)
- *Auditors*' comments (how conduct of audit went)
- Appendix A – Details for each requirement which kind of evidence is to be considered as sufficient by a testing laboratory.

REQ-#	Requirement	Result	Auditor remarks
REQ-01	Security by Design	C / NC	
REQ-02	Version Control	C / NC	C: no comment C+: a robust VC system is there and access control to individuals is maintained strictly and timely C-: version control is not applied in all cases NC: not documented; only some docs are controlled in there; processes are not clear; no individual user accounts
REQ-03	Change Tracking	C / NC	
REQ-04	Source Code Review	C / NC	- comment
REQ-05	Software Security Testing	C / NC	+ comment
REQ-06	Staff Education		
REQ-07	Vulnerability Remedy Process		
REQ-08			

REQ-#	Requirement	Result	Auditor remarks
REQ-09			
REQ-10			
REQ-11			
REQ-12			
REQ-13			
REQ-14			
REQ-15			
REQ-16			
REQ-17			

Annex C Document Management

C.1 Document History

Version	Date	Brief Description of Change	Editor / Company
1.0	<approval date>	Initial Creation by SECAG	
0.21	16.6.2016	Amended text during SECAG#15c meeting	John Hickey/Nokia
0.20	14.6.2016	Added text to 9.1.8., added 9.2.1 and changed Annex A editor note.	John Hickey/Nokia
0.19	7.6.2016	Added note to 9.1.8 on how NESAS differs to other schemes.	John Hickey/Nokia
0.18	19.3.16	Final draft produced after SECAG#13	James Moran, GSMA
0.17	15.3.2016	Updated during SECAG#13	Sven Lachmund / Deutsche Telekom Martin Peylo / Nokia Networks
0.16	21.1.2016	During SECAG#11: - Added text on the Audit Certificate - Inserted editor's note indicating the need to clarify who gets access to the Audit Report and who in the end grants the accreditations. - Term improvements throughout the document	Martin Peylo / Nokia Networks
0.15	20.1.2016	Added text/changes agreed on Guidelines and Evidence during SECAG#11.	Martin Peylo / Nokia Networks
0.14	4.1.2016	Updated with result of SECAG#10: - Changes discussed during the meeting (SECAG Doc 10_011) - CR by Deutsche Telecom as discussed (SECAG Doc 10_005 Rev 1) Minor editorial improvements throughout the resulting document.	Martin Peylo / Nokia Networks
0.13	17.11.2015	Proposed version was sent to SECAM list for email approval; approved on 24.11.	Martin Peylo / Nokia Networks
0.12	3.9.2015	Updated with result of SECAG#8	Martin Peylo / Nokia Networks
0.11	28.5.2015	Editorial improvements throughout the document; NESAG->SECAG, harmonized style, fixed grammar and spelling, fixed references, etc.	Martin Peylo / Nokia Networks
0.10	5.5.2015	Updated with result of SECAG#3	Martin Peylo / Nokia Networks

0.9	12.2.2015	Updated with result of SECAG#1	Martin Peylo / Nokia Networks
0.8	12.12.2014	Updated with result of WG2 call 3. Additional minor editorial fixes.	Martin Peylo / Nokia Networks
0.7	10.12.2014	Updated with result of NESAG#10 discussions	Martin Peylo / Nokia Networks
0.6	29.10.2014	Updated with result of NESAG#9 discussions. Few minor editorial changes throughout the whole document.	Martin Peylo / Nokia Networks
0.5	9.10.2014	Updated with result of WG2 call 2	Martin Peylo / Nokia Networks
0.4	25.9.2014	Updated with result of WG2 call 1	Martin Peylo / Nokia Networks
0.3	17.9.2014	Updates during NESAG#8, plus additional editorial changes as discussed during NESAG#8	Martin Peylo / Nokia Networks
0.2	28.6.2014	Updated during NESAG#6	Martin Peylo / NSN
0.1vision	29.4.2014	initial creation	Martin Peylo / NSN

C.2 Other Information

Type	Description
Document Owner	NESAS Accreditation Board, SECAG subgroup of FASG
Editor / Company	XXX, GSMA

It is our intention to provide a quality product for your use. If you find any errors or omissions, please contact us with your comments. You may notify us at <XXX@gsma.com>. Your comments or suggestions & questions are always welcome.

Editor's note: Above reference to the document editor and the email address of the NESAS Accreditation Board need to be inserted before release of version 1.0 of the document.