Network Equipment Security Assurance Scheme – Development and Lifecycle Security Requirements

Version 1.1

20 July 2020

This is a Non-binding Permanent Reference Document of the GSMA

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 – Network Equipment Security Assurance Scheme - Overview [1].

This document defines security requirements for an Equipment Vendor's Development and Product Lifecycle Processes.

NESAS is governed by the provisions set out in FS.14, FS.15 and FS.16. In case of any conflict between those documents and any other provisions in other NESAS documentation, save for Section 3.6 in FS.13, the provisions in FS.14, FS.15 and FS.16 shall prevail.

1.1 Scope

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

The number of requirements is kept relatively small 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.

The procedure to run an audit is described in FS.15 [2].

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 network operators and Equipment Vendors.

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.

2 Definitions

2.1 Common Abbreviations

Term	Description
3GPP	The 3rd Generation Partnership Project
CPA	Commercial Product Assurance
FASG	Fraud and Security Group
NCSC	National Cyber Security Centre
NESAS	Network Equipment Security Assurance Scheme
NIST	National Institute of Standards and Technology
PDF	Portable Document Format

[1] Compare to NCSC's CPA build standard [5] is seen as inspiration for the abstraction level, amount, and content of the requirements.

Term	Description
SCAS	Security Assurance Specification
SECAG	Security Assurance Group
SHA-512	Secure Hash Algorithm-512
TR	3GPP Technical Report
TS	3GPP Technical Standard

2.2 Glossary

Unless defined below all capitalised terms shall have the same meaning as in FS13:

Term	Description
Audit Guidelines	Document giving guidance to the Auditor and Equipment Vendor on how to interpret the requirements.
Audit Report	Document presenting the results of the audit conducted at the Equipment Vendor by the Auditor.
Audit Summary Report	A subset of the Audit Report created by the Auditor that summarises the key results.
Auditor	Organisation appointed and contracted by GSMA and selected by Equipment Vendor to conduct audits of Vendor Development and Product Lifecycle processes.
Conformance Claim	A written statement by the Equipment Vendor that confirms it meets the NESAS security requirements for the Development and Product Lifecycle Processes that are to be assessed.
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.
NESAS Oversight Board	The body overseeing NESAS, run by the GSMA. It is responsible for the governance of the Vendor Development and Product Lifecycle Process assessments and quality assurance of NESAS.
NESAS Security Test Laboratory	A test laboratory that is ISO/IEC 17025 accredited in the context of NESAS and that conducts Network Product evaluations. It can be owned by any entity.
Network Product	Network equipment produced and sold to network operators by an Equipment Vendor.
Network Product Class	In the context of NESAS, the class of Network Products that all implement a common set of 3GPP defined functionalities.
Network Product Development Process	The stages through which Network Products journey throughout their development including planning, design, implementation, testing, release, production and delivery.
Network Product Lifecycle Processes	The stages through which developed Network Products journey to end of life including maintenance and update releases during their lifetime.

Term	Description
Release	Version of a Network Product being made available for deployment. The first Release of a Network Product is 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 [6], 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]	FS.15 -– Network Equipment Security Assurance Scheme – Vendor Development and Product Lifecycle Assessment Methodology
[3]	"Key words for use in RFCs to Indicate Requirement Levels", S. Bradner, March 1997. http://www.ietf.org/rfc/rfc2119.txt
[4]	3GPP TR 33.916, "Security assurance scheme for 3GPP Network Products for 3GPP Network Product classes". http://www.3gpp.org/DynaReport/33916.htm
[5]	"CPA Build standard", contains the NCSC's requirements for a Network Product developer's security engineering approach. https://www.ncsc.gov.uk/content/files/protected_files/document_files/The%20CPA%20Build%20Standard%201.3.pdf
[6]	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
[7]	NIST FIPS PUB 180-4 "Secure Hash Standard (SHS)", August 2015. http://dx.doi.org/10.6028/NIST.FIPS.180-4
[8]	SEI CERT Coding Standards, Carnegie Mellon University, https://wiki.sei.cmu.edu/confluence/display/seccode/SEI+CERT+Coding+Standards.

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 [3]."

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 lifetime of a Network Product.

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

3.2 Network Product Development Process

The Network Product development phases are as follows:

#	Phase	Description
1.	Planning	In case of a completely new Network Product, the requirements for the first Release are planned. In the case of a new version of an existing Network 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 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 Network Product. In the 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 1: Product Development Process

For new Network Products and any modifications of Network Products, the Product Development phases are executed in a cyclical fashion, starting again from the beginning once finished for the previous Network Product release.

3.3 Network Product Lifecycle Processes

The Product Lifecycle in the NESAS context covers all activities from the initial Network Product idea to end of life. It consists of a number of processes, as follows:

Process	Description
Product development process	As outlined in Section 3.2 above.
First Commercial Introduction	The Network Product starts its commercial lifetime by means of a first Release to be accepted for use in live commercial networks. Before that, earlier Releases may have been tested in test environments.
Update	The Network Product is updated by means of either a minor or a major Release. This phase is usually a cycle of such Releases.
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.
Major Release	A major Release fixes vulnerabilities and other bugs found in earlier versions. It may introduce major feature enhancements and architectural changes.
End Of Life	No updates for the Network Product are supplied anymore. As this process occurs after contractual and regulatory requirements to maintain the Network Product have ceased, this commonly marks the end of a Network Product's lifetime.

Table 2: Product Lifecycle Processes

4 Assets

4.1 Introduction

The ultimate goal of security related elements in the Vendor Development and Product Lifecycle Process is to ensure that the interests of the mobile network operator and its customers are protected. Usually, the main interest of the network operator is the flawless operation of its network. This section defines, discusses and prioritises 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 and Product Lifecycle Process. The assets need to be protected from threats that could exploit vulnerabilities in the Network Product during its lifecycle. Protection of relevant assets needs to be in place during the whole lifetime of a Network Product.

Security objectives in section 6 are derived from the assets and from identified relevant threats are defined in section 5.

The identified relevant assets are described in the following subsections.

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. Source code includes application software as well as software and hardware platforms and integrated APIs if any. Software platforms include operating systems and virtualisation management software.

Common types of source code include those:

- Created by the Equipment Vendor dedicated for use in one or more particular Network Products **[SRC_VND]**
- Created by a subcontracting 3rd party on behalf of the Equipment Vendor dedicated for use in one or more particular Network Products **[SRC_SUB]**
- Created as general software elements (e.g. libraries) by a 3rd party supplier and provided to the Equipment Vendor as binary **[SRC_TRB]**
- Created as general software elements (e.g. libraries) by a 3rd party supplier and provided to the Equipment 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.

Each Network Product contains a combination of multiple software packages after manufacturing.

Common types of Software Packages include those:

- Created by the Equipment Vendor **[SPK_VND]**
- Created by a subcontracting 3rd party on behalf of the Equipment 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 elements integrating the whole Network Product **[FIN_HWR]**, typically including a certain release of FIN_SWR after the production process.

4.5 Security Documentation (DOC)

Security documentation is used to guide Network Product design and development of source code and is a deliverable during the Network Product design and development process.

A common type of security document includes that created by the Equipment Vendor during the Network Product design and development process, e.g. schematics or architecture design documents. **[DOC_DES]**

4.6 Operated Products (OPP)

Operated Network Products are those that are in active use by a mobile network 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 Equipment Vendor.

- Network Products operated in live networks **[OPP_LVE]**

4.7 Product Development Support System (SUP)

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

Common types of support system:

- Product build environment, including compilation environment and tools used in the Network 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 is focussed on identifying those threats that introduce the highest level of risk.

5.2 Threat Descriptions

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

Threat	Assets	Description
T_ROGUE_DEV	SRC_VND SRC_SUB	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	Source code dedicated for use in the Network Product leads to a vulnerability.
T_VULN_SRC_OTHER	SRC_TRB SRC_TRS SRC_FOS	General source code by a third party leads to a vulnerability.

Threat	Assets	Description
T_POOR_DES	FIN_SWR FIN_HWR OPP_LVE	A design flaw of the Network Product leads to a vulnerability. Lacking/insufficient security considerations in architecture or design of the Network 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_LVE	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	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	An operator is not aware 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	An Equipment Vendor does not become aware of vulnerabilities caused by used 3rd party components.
T_VULN_NOHANDL	SPK_VND SPK_SUB FIN_SWR	Vulnerability found by Equipment Vendors, operators, or other 3rd party, and made known to the Equipment Vendor is not appropriately handled.
T_SENSITIVE_DOC_LEAK	DOC_DES	Security documents containing sensitive information about the Network Product are leaked. This could be utilised by malicious attackers to find out vulnerabilities and launch related attacks.
T_BLDTOOL_TAMPER	SUP_BUI	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	The customer documentation for the Network Product does not cover the actual functionality and properties of the Network Product.
T_NO_CONTACT	OPP_LFE	The customer operator has no, or not the right, contact at the Equipment Vendor organisation to address any security inquiries or incidents.

Threat	Assets	Description
T_VULN_SWR2	FIN_SWR	A vulnerability that exists in multiple places of the software or different branches of the software is not patched in all places.
T_TPC_EOL	FIN_SWR FIN_HWR	Third party components, including libraries, operating systems and tools may cease to be supported, or have major change to its support structure, thus not receiving any updates to counter security vulnerabilities.

Table 3: Threat Descriptions

6 Security Objectives

6.1 Introduction

The Equipment Vendor that wishes to subject its processes to assessment and audit 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 network 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 Vendor Development and Product Lifecycle Processes.

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 T_VULN_SWR2 T_TPC_EOL	To reduce the window of opportunity originating from a known vulnerability.

Identifier	Objective	Threats	Description
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 T_TPC_EOL	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 used 3rd party components are identified as early as possible.	T_VULN_UNAWARE	To ensure that known vulnerabilities can be mitigated for operated 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 Network 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 Network 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

Identifier	Objective	Threats	Description
			secure design of the Network Product.
O_SEC_TEST	Testing demonstrates secure and robust implementation of the Network Product.	T_ROGUE_DEV T_POOR_DES	During testing of the Network 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 aware of IT/network security matters.	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 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 Equipment Vendor organisation.	T_NO_CONTACT	There is a clear communication from the Equipment Vendor to its operator customers to let operators know who to contact for any security inquiries or incidents.

Identifier	Objective	Threats	Description
O_CONT_IMP	Reduce the likelihood of vulnerabilities re-occurring by continual improvement	T_POOR_DES	Security issues that had been identified are analysed to determine how to prevent them from reoccurring.

Table 4: Security Objectives for the Vendor Development and Product Lifecycle Processes

7 Security Requirements

7.1 Introduction

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

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

The requirements of this 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 to achieve the same security objective.

7.2 Design

7.2.1 [REQ-01] Security by Design

[Requirement Text: The Network Product shall implement security by design throughout the whole development and product lifecycles. Therefore, architecture and design decisions shall be made based on a set of security principles that are tracked throughout the development and product lifecycles.] **[O_TRA_ANALYSE]**

The goal of security by design is to limit the impact of security risks through robust and consistently applied principles such as (but not limited to):

- Security architectural principles:
    - Domain separation
    - Layering
    - Encapsulation
- Security design principles:
    - Least privilege

- Attack surface minimisation
- Centralised parameter validation & centralised security functionality
- Preparing for error & exception handling
- Privacy by design

Security principles such as the above should be considered and applied when appropriate.

In the design phases, a threat analysis process for the Network Product shall be undertaken to identify the potential threats and related mitigation measures.

7.3 Coding

7.3.1 [REQ-04] Source Code Review

[Requirement Text: The Equipment Vendor shall ensure that new and changed source code dedicated for a Network Product is appropriately reviewed in accordance with an appropriate coding standard. If feasible, the review should also be implemented by means of utilising a Source Code Analysis Tool and automation where appropriate.] **[O_VUL_INT]**

The goal is to help reduce the risk of software issues that could introduce vulnerabilities in the Network Product. An example of a best practice coding standard is Carnegie-Mellon, SEI CERT [8].

7.3.2 [REQ-18]: Source Code Governance

[Requirement Text: The Equipment Vendor shall ensure that no changes are introduced into the Network Product without appropriate governance.] **[O_CONTROL]**

The goal is to prevent unauthorised changes and reduce the likelihood of unintended or unauthorised changes. It is also to ensure that there are independent lines of control for any changes.

7.4 Compilation

7.4.1 [REQ-10] Automated Build Process

[Requirement Text: The Equipment vendor shall utilise an automated build tool with a minimum of manual intervention to compile the source code and store the build logs.] **[O_PROT_BLDTOOL]**

The goal is to ensure that the build is reproducible, deterministic and that it covers the security procedures defined by the Equipment Vendor.

7.4.2 [REQ-11] Build Environment Control

[Requirement Text: 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]**

The goal is to ensure that the same binaries can be reproduced and that there is a clear audit trail for any modifications.

7.5 Testing

7.5.1 [REQ-05] Security Testing

[Requirement Text: Security testing should include the validation of security functionality, both positive and negative testing, as well as vulnerability testing of the Network Product.

Network Products are to be tested from a security perspective within a fair representation of the operational environment.

Vulnerability testing shall test for the robustness of the Network Product against undefined/unexpected input.] **[O_VUL_INT], [O_SEC_TEST]**

The goal is to ensure that security functionality has been validated and that potential vulnerabilities are detected and mitigated before the Network Product is delivered.

7.6 Release

7.6.1 [REQ-13] Software Integrity Protection

[Requirement Text: The Equipment Vendor shall establish and maintain methods to ensure that the delivery of Network Products is carried out under controlled conditions. The mobile network operator shall be provided with appropriate means to identify whether a received software package is genuine.] **[O_GENUINE_SWR]**

The goal is for mobile network operators to be able to check the integrity of the software package and associated documentation.

7.6.2 [REQ-14] Unique Software Release Identifier

[Requirement Text: All released software package versions shall bear a unique identifier that maps to a specific build version.] **[O_IDENT_SWR]**

The goal is to ensure that all software is identifiable and that the exact same software uses the same unique identifier.

7.6.3 [REQ-16] Documentation Accuracy

[Requirement Text: 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]**

The goal is to ensure that the Network Product documentation reflects the version of the Network Product delivered.

7.6.4 [REQ-20] Security Documentation

[Requirement Text: The documentation delivered with the Network Products contains all up-to-date information necessary to securely configure and run the Network Product.] **[O_ACCURATE_DOC]**

The goal is to ensure that operators can configure the Network Products in a secure way, including clarifying if the default configuration is secure.

7.7 Operation

7.7.1 [REQ-17] Security Point of Contact

[Requirement Text: The Equipment Vendor shall provide a point of contact for security questions/issues and communicate this point of contact to its customers and 3rd party vulnerability disclosers. This point of contact shall be able to find the right person/department inside the Equipment Vendor organisation to deal with security concerns raised by a customer/3rd party vulnerability discloser.] **[O_SEC_POC]**

The goal is to ensure that the Equipment Vendor forwards incoming requests to the relevant department in a timely and secure manner and that the requesting or informing party receives a timely and appropriate response.

7.7.2 [REQ-12] Vulnerability Information Management

[Requirement Text: The Equipment 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]**

The goal is to reduce the impact on the Network Product of 3rd party components becoming unsupported, unavailable or vulnerable.

7.7.3 [REQ-07] Vulnerability Remedy Process

[Requirement Text: The Equipment Vendor shall establish a process to deal with vulnerabilities found in, or in relation to, released Network Products (including 3rd party components). Vulnerabilities shall be dealt with appropriately and, if applicable, patches/software upgrades shall be distributed to all affected mobile network operators, in order to honour existing maintenance contracts within an agreed schedule.] **[O_VUL_PAT]**

The goal is to reduce the impact on the Network Product becoming vulnerable or 3rd party components becoming unsupported, unavailable or vulnerable.

Note: Mitigating 3rd party software that has become unsupported will be dealt with in a future release.

7.7.4 [REQ-08] Vulnerability Remedy Independence

[Requirement Text: For ease of deployment, the Equipment Vendor shall have the facility to provide patches/software upgrades that close security vulnerabilities independently from unrelated patches/software upgrades that modify functionality of the Network Product.] **[O_VUL_PAT]**

The goal is to ensure that security remedies can be delivered swiftly and independently from the functional delivery schedule.

7.7.5 [REQ-15] Security Fix Communication

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

The goal is to ensure that mobile network operators are informed in a timely way to apply any security fixes**.**

7.8 General Requirements

7.8.1 [REQ-02] Version Control System

[Requirement Text: During the entire lifetime of a Network Product, the Equipment Vendor shall utilise a version control system on hardware, source code, build tools and environment, binary software, 3rd party components, and customer documentation ensuring accountability, authorisation and integrity of all changes.] **[O_CONTROL]**

The goal is to be able to trace all the above elements together in a finished Network Product.

7.8.2 [REQ-03] Change Tracking

[Requirement Text: The Equipment Vendor shall establish a comprehensive, documented and cross Network Product line procedure to ensure that all requirements and design changes, which may arise at any time during the development and product lifecycles and which impact the Network Product(s) (this includes all aspects of requirement 7.3.1.), are managed and tracked in a systematic and timely manner appropriate to the life cycle stage of all affected product components in all Network Products.] **[O_CONTROL]**

The goal is to ensure that all changes are made in a consistent way through the development of all affected Network Product components in all Network Products.

7.8.3 [REQ-06] Staff Education

[Requirement Text: Continuous education of all staff involved in Network Product design, engineering, development, implementation, testing and maintenance shall be provided to ensure knowledge and awareness on security matters, relevant to their roles are up-to-date.] **[O_STAFF_EDU]**

The goal is to ensure that all staff have knowledge and awareness on security matters relevant to their role, maintained to a consistently high level.

7.8.4 [REQ-09] Information Security Management

[Requirement Text: In the entire lifecycle, the Equipment Vendor shall employ an information classification and handling scheme to avoid sensitive information, such as security flaws, signing keys, etc., being leaked.] **[O_PROT_DOC]**

The goal is to ensure that sensitive information is identified, classified and managed appropriately.

7.8.5 [REQ-19] Continual Improvement

[Requirement Text: The Equipment vendor must have a continual improvement process for its development and product lifecycle and this process must include a root cause analysis of the security flaws. The resulting improvements shall be incorporated into the relevant design or processes.] **[O_CONT_IMP]**

The goal is to improve processes and to reduce the likelihood of vulnerabilities re-occurring by continual improvement.

Annex A Document Management

A.1 Document History

Version	Date	Brief Description of Change	Editor / Company
1.0	Sep 2019	Release 1 approved by SECAG	James Moran / GSMA
1.1	Aug 2020	Regrouping & reordering of security requirements	James Moran / GSMA

A.2 Document and NESAS Release Mapping History

Document Version	Applicable NESAS Release
1.0	NESAS 1.0
1.1	NESAS 1.1

A.3 Other Information

Type	Description
Document Owner	GSMA, SECAG
Editor / Company	James Moran, 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 nesas@gsma.com. Your comments or suggestions