Network Equipment Security Assurance Scheme – Security Requirements for Vendor Development and Product Lifecycle Processes

Version 3.0

20 February 2025

Security Classification: Non-Confidential

Copyright Notice

Disclaimer

Compliance Notice

The information contain herein is in full compliance with the GSMA Antitrust Compliance Policy.

This Permanent Reference Document is classified by GSMA as an Industry Specification, as such it has been developed and is maintained by GSMA in accordance with the provisions set out GSMA AA.35 - Procedures for Industry Specifications.

Contents

Licensing Statement

This GSMA document and its content is:

1. the exclusive property of the GSMA; and
2. provided "as is", without any warranties by the GSMA of any kind.

Foreword

This Technical Specification was produced by the GSM Association.

The contents of the present document are subject to continuing work within the GSMA NESAS Group and can change following formal GSMA approval. When the NESAS Group modify the contents of the present document, it will be re-released by the GSMA with an identifying change of release date and an increase in version number as follows:

Version x.y.

where:

x the first digit is incremented for all major changes

y the second digit is incremented for all changes of corrections, technical enhancements, updates, etc.

Modal verbs terminology

In the present document, modal verbs have the following meanings:

shall indicates a mandatory requirement to do something

shall not indicates an interdiction (prohibition) to do something

"**shall**" and "**shall not**" are confined to the context of normative provisions.

"**must**" and "**must not**" are not used as substitutes for "**shall**" and "**shall not**".

should indicates a recommendation to do something

should not indicates a recommendation not to do something

may indicates permission to do something

need not indicates permission not to do something

"**may not**" is ambiguous and is not used in normative elements.

can indicates that something is possible

cannot indicates that something is impossible

The constructions "**can**" and "**cannot**" are not substitutes for "**may**" and "**need not**".

will indicates that something is certain or expected to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

will not indicates that something is certain or expected not to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

Introduction

The present document defines security requirements for an Equipment Vendor's Development and Product Lifecycle Processes. The present document forms part of the documentation of the Network Equipment Security Assurance Scheme (NESAS), which is described in the NESAS Framework document GSMA PRD FS.13 [1].

NESAS is governed by the provisions set out in GSMA PRD FS.14 [3], GSMA PRD FS.15 [4] and GSMA PRD FS.16 (the present document). In case of any conflict between those documents and any other provisions in other NESAS documentation, save for clause 3.8 in GSMA PRD FS.13 [2], the provisions in GSMA PRD FS.14 [3], GSMA PRD FS.15 [4] and GSMA PRD FS.16 (the present document) shall prevail.

NESAS was originally created by GSMA and responsibility for its maintenance and development of the NESAS specifications rests with the NESAS Group, which comprises representatives from mobile telecom network operators, infrastructure and equipment vendors, security auditors and test laboratories. The NESAS Group is an Industry Specification Issuing Group, and as such, it is bound to GSMA PRD AA.35 [1] governance.

The NESAS Group is responsible for maintaining the NESAS specifications and for facilitating periodic reviews involving all relevant stakeholders.

The Scheme Owner using NESAS specifications can add additional documentation and will be responsible for development and maintenance of its own documents.

1 Scope

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

When defining the requirements in the present document internationally recognised best practices were followed. The number of requirements is kept relatively small to keep evaluation costs reasonable and to focus on critical controls. They are complemented by requirements in SCASes adopted by the Scheme Owner in accordance with GSMA PRD FS.62 [4].

The procedures to perform an Audit are defined in GSMA PRD FS.15 [4].

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: Hyperlinks included in this clause were valid at the time of publication,

The following referenced documents are necessary for the application of the present document.

[1] GSMA PRD AA.35: "Procedures for Industry Specifications"

[2] GSMA PRD FS.13: "Network Equipment Security Assurance Scheme – Framework"

[3] GSMA PRD FS.14: "Network Equipment Security Assurance Scheme – Requirements for NESAS Auditing Organisations, Security Test Laboratories, and Associated Personnel"

[4] GSMA PRD FS.15: "Network Equipment Security Assurance Scheme – Assessment Methodology for Vendor Development and Product Lifecycle Processes"

[5] GSMA PRD FS.62: "Network Equipment Security Assurance Scheme – Adoption Procedure for Security Assurance Specifications"

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: Hyperlinks included in this clause were valid at the time of publication,

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] Carnegie Mellon University: "SEI CERT Coding Standards", https://wiki.sei.cmu.edu/confluence/display/seccode/SEI+CERT+Coding+Standards

[i.2] NIST SP 800-30 Rev. 1 2012: "Guide for Conducting Risk Assessments", http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the following terms apply:

3rd Party Component: Object with discrete structure, such as an assembly, a software package, which is sourced from an external entity and incorporated into a Network Product.

Audit: A review and assessment that is performed and completed by an Audit Team against the NESAS Development and Product Lifecycle Security Requirements following the NESAS assessment methodology.

Equipment Vendor: Organisation that develops, maintains and supplies network equipment that supports functions defined by 3GPP or another SDO.

NESAS Development and Product Lifecycle Security Requirements: The security requirements that Vendor Development and Product Lifecycle Processes comply with under NESAS and against which Audits are performed.

NESAS Group: The Industry Specification Issuing Group of the GSMA that is tasked with the overall implementation, governance, maintenance and further development of NESAS specifications.

NESAS Security Test Laboratory: A test laboratory that is authorised to perform Network Product Evaluations and Evidence Evaluations under NESAS.

Network Function: A defined processing function in a network, which has defined functional behaviour and defined interfaces.

Network Product: Network Equipment developed, maintained and supplied by an Equipment Vendor, consisting of one or more Network Function(s).

Network Product Class: A class of products that implements a common set of functionalities.

Release: Version of a Network Product being made available for deployment.

Scheme Owner: Organisation or authority responsible for developing, maintaining or operating a specific security assurance or certification scheme that uses the NESAS specifications.

Software: Physically intangible set of instructions, defined in a formal language, written in digital format.

Vendor Development and Product Lifecycle Processes: The stages through which Network Products journey throughout their development including planning, design, implementation, testing, release, production and delivery and the stages to end of life including maintenance and update releases during their lifetime.

Vendor Development Process: Stages through which Network Products journey throughout their development including planning, design, implementation, testing, release, production and delivery.

Vendor Product Lifecycle Processes: Stages through which developed Network Products journey to end of life including maintenance and update releases during their lifetime.

Vulnerability: 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.

NOTE: The term "Vulnerability" is as defined by NIST in NIST SP 800-30 Rev. 1 2012 [i.2].

3.2 Symbols

Symbols are not applicable in the present document.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

3GPP	The 3rd Generation Partnership Project
GSMA	GSM Association
ISAG	Industry Specification Approval Group
NESAS	Network Equipment Security Assurance Scheme
NIST	National Institute of Standards and Technology
PRD	Permanent Reference Document
SCAS	Security Assurance Specification
SEI	Software Engineering Institute

4 Definition of Vendor Development and Product Lifecycle

4.1 Introduction

Protection of relevant assets, as defined in clause 5, 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 clause 8 are designed to mitigate the relevant threats defined in clause 6 and are to be implemented within the Vendor Development and Product Lifecycle defined within this clause.

4.2 Vendor Development Process

The development phases in the Vendor Development Process are as follows:

Table 1: Vendor Development Process

#	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 and Building	The planned requirements are implemented as per the design and the Network Product is built.
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 and Building" 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.

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.

4.3 Vendor 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:

Table 2: Vendor Product Lifecycle Processes

Process	Description
Vendor Development Process	As outlined in clause 4.2 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.

Process	Description
	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.

5 Assets

5.1 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 clause 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 the present document are the Network Product and its constituent parts that exist during the Vendor Development and Product Lifecycle Processes. 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 clause 7 are derived from the assets and from identified relevant threats are defined in clause 6.

The identified relevant assets are described in the following sub-clauses.

5.2 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]**

5.3 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]**

5.4 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.

5.5 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]**

5.6 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]**

5.7 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]**

6 Threats and their Risks

6.1 Introduction

This clause 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.

6.2 Threat Descriptions

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

Table 3: Threat Descriptions

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 3rd 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_BLD_TAMPER	SUP_BUI	A malicious attacker can 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_LVE	The customer documentation for the Network Product does not cover the actual functionality and properties of the Network Product.
T_NO_CONTACT	OPP_LVE	The customer operator has no, or not the right, contact at the Equipment Vendor organisation to address any security inquiries or incidents.
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	Support of 3rd Party Components, including libraries, operating systems and tools can stop, or have major change to its support structure, thus preventing updates to counter security Vulnerabilities.

7 Security Objectives

7.1 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 shall 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.

Clause 7.2 lists the security objectives for the Vendor Development and Product Lifecycle Processes.

7.2 Security Objectives

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

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.

Identifier	Objective	Threats	Description
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.
O_PROT_DOC	Sensitive documents do not leak.	T_SENSITIVE_DOC_LEAK	To protect sensitive information from becoming known to potential attackers.
O_PROT_BLD	Compilation and build environment is protected from tampering.	T_BLD_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 can 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 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.

Identifier	Objective	Threats	Description
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.
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.
O_SPC_SEC	Ensure the quality and availability of 3rd Party Components.	T_VULN_SRC_OTHER T_VULN_UNAWARE T_VULN_NOHANDL	To lower the risk of integrating vulnerable, unsupported 3rd Party Components into Network Products.

8 Security Requirements

8.1 Introduction

In order to have sufficient confidence in the Vendor Development and Product Lifecycle Processes, certain security requirements shall be met.

These requirements, which are outlined below, 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 objectives, while one or more requirements may exist to fulfil the same security objective.

The requirements of the present document 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 the following clauses to achieve the same security objective.

8.2 Design

8.2.1 [REQ-DES-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:
  - Security by default
  - 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 performed to identify the potential threats and related mitigation measures, also taking into consideration the interaction with other network equipment and entities, as well as the impact the Network Product has on the network regarding security.

8.3 Implementation

8.3.1 [REQ-IMP-01] 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 [i.1].

8.3.2 [REQ-IMP-02]: 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.

8.4 Building

8.4.1 [REQ-BUI-01] Automated Build Process

[Requirement Text: The Equipment Vendor shall utilise an automated build process with a minimum of manual intervention to build the Software of the finished product and store the build logs.] **[O_PROT_BLD]**

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

8.4.2 [REQ-BUI-02] Build Process Management

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

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

8.5 Testing

8.5.1 [REQ-TES-01] Security Testing

[Requirement Text: Security testing shall include the validation of security functionality (both positive and negative testing as applicable), as well as Vulnerability testing of the Network Product.

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

Principles applied in the Security by Design requirement should be tested to ensure the appropriate implementation of those principles and functions.

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 weaknesses that could lead to potential Vulnerabilities are detected and mitigated before the Network Product is delivered.

8.6 Release

8.6.1 [REQ-REL-01] 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.

8.6.2 [REQ-REL-02] 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.

8.6.3 [REQ-REL-03] 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.

8.6.4 [REQ-REL-04] Security Documentation

[Requirement Text: The documentation delivered with the Network Products shall contain all up-to-date information necessary to securely configure and operate the Network Product. Default configuration of the product should be explicitly presented in the security documentation.] **[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.

8.7 Operation

8.7.1 [REQ-OPE-01] 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.

8.7.2 [REQ-OPE-02] 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.

8.7.3 [REQ-OPE-03] 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 assessed and dealt with according to this process 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.

8.7.4 [REQ-OPE-04] 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.

8.7.5 [REQ-OPE-05] 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**.**

8.8 General Requirements

8.8.1 [REQ-GEN-01] 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.

8.8.2 [REQ-GEN-02] 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 can arise at any time during the development and product lifecycles and which impact the Network Product(s) (this includes all aspects of requirement REQ-GEN-01.), 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.

8.8.3 [REQ-GEN-03] 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.

8.8.4 [REQ-GEN-04] Information Classification and Handling

[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.

8.8.5 [REQ-GEN-05] Continual Improvement

[Requirement Text: The Equipment Vendor shall have a continual improvement process for its development and product lifecycle and this process shall 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.

8.8.6 [REQ-GEN-06] Sourcing and Lifecycle Management of 3rd Party Components

[Requirement Text: The Equipment Vendor shall have processes in place to ensure the quality of 3rd Party Components during the product lifecycle. The Equipment Vendor shall select supported 3rd Party Components and shall avoid using those reaching the end of life.] **[O_SPC_SEC]**

The goal is to decrease the possibility of the Equipment Vendor sourcing and using vulnerable, tainted and unsupported 3rd Party Components within its supply chain.

History

Document history		
Version	**Date**	**Brief Description of Change**
1.0	Sep 2019	Release 1 approved by NESASG
1.1	Aug 2020	Regrouping & reordering of security requirements
2.0	Feb 2021	New security requirement on third party components added to the scheme. A re-grouping and re-numbering of all requirements has also been undertaken.
2.1	Jan 2022	Removal of references to NESAS releases. Addition of provisions pertaining to the licensing of NESAS documentation. Title of REQ-GEN-04 changed to better match requirement text. Correction of an incorrect reference to another requirement in REQ-GEN-02, now pointing to the correct requirement. Updated sction 7.4, objective O_PROT_BLD and threat T_BLD_TAMPER to reflect that these address the build process in the broadest possible sense, and are not only limited to build tools/build environment.
2.2	Oct 2022	Security requirements updated to include security by default, end to end threat analysis, third party component maintenance and secure configuration.
2.3	Sep 2023	Definitions updated to align with other scheme documents and updates made pertaining to NESAS Group and reference to SCAS development guidelines and GSMA adoption process added. This document update is not material to the scheme and does not require vendors to undergo an audit to maintain the validity of their NESAS status.
3.0	Feb 2025	Clarity of descriptions and consistent use of terms improved. Definitions updated. Separation of NESAS specifications from scheme run by GSMA. Details of GSMA NESAS have moved to FS.51.