NESAS - Product and Evidence Evaluation Methodology
Version 1.0
20 February 2022

This is a Binding Permanent Reference Document of the GSMA

Security Classification: Non-confidential

Copyright Notice

Disclaimer

Compliance Notice

The information contain herein is in full compliance with the GSM Association's 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 in GSMA AA.35 - Procedures for Industry Specifications.

Table of Contents

1 Introduction

This document describes the Network Equipment Security Assurance Scheme (NESAS) product and evidence evaluation methodology.

1.1 Scope

The evaluation methodology establishes how the product and evidence evaluation is done at the procedural and operational level. It is provided to assist the Equipment Vendor and the NESAS Security Test Laboratory in the performance of those activities.

1.2 Document Maintenance

NESAS was originally created and developed under the supervision of GSMA's Security Assurance Group (SECAG) that comprised of representatives from mobile telecom network operators, infrastructure vendors, security auditors and test laboratories.

The scheme owner is responsible for maintaining NESAS and for facilitating periodic reviews involving all relevant stakeholders.

1.3 Definitions

Term	Description
Applicant	legal entity asking for certification Note: The Applicant role is usually fulfilled by the equipment vendor.
Audit Report	document presenting the results of the audit conducted at the equipment vendor by the Audit Team
Audit Summary Report	subset of the Audit Report created by the Audit Team that summarises the key results
Audit Team	collective group of Auditors, generally to consist of two or more people, that undertake a Vendor Development and Product Lifecycle Processes audit
Auditor	individual that is qualified to perform Vendor Development and Product Lifecycle Processes audits and makes up part of the Audit Team Note: This definition does not mandate a certain employer for the Auditor, which is possibly employed by a dedicated "audit company" or by a CB (or could be freelancers) and the qualification is ensured by the certification of said individuals.
Certification Body	body that performs certification activities corresponding to the accreditation(s) received by the National Accreditation Body and to the authorisation(s) received by the NCCA
Compliance Evidence	evidence to be provided by the Applicant to the Certification Body, demonstrating that the Applicant applied its previously independently audited development and lifecycle processes to build the Product under Evaluation Note: An Auditor defines in the Audit Report which Compliance Evidence is required for subsequent product evaluations
Elements for Assessment	technical documentation, and all other relevant information, relating to the scope of the planned assessment
Evaluation Report	documented assessment produced by the NESAS CCS accredited Testing Laboratory of the level of compliance of a Network Product with the relevant Security Assurance Specification(s)

Term	Description
Network Product	network equipment produced and sold to network operators by an equipment vendor
Network Product Development Process	stages through which developed Network Products journey throughout their development including planning, design, implementation, testing, release, production and delivery
Network Product Lifecycle Process	stages through which developed Network 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. Note: The first Release of a Network Product is assumed to be a new Network Product
Product under Evaluation	the product for which a certificate is sought by the Applicant
Security Assurance Specification	specification containing security requirements and test cases for a dedicated network function or a group of network functions
Software	physically intangible set of instructions, defined in a formal language, written in digital format Note: Software is used by a machine to be interpreted or executed. It can exist in various formats, such as binary software, which is only machine-readable, and scripts and source code, which is human readable and/or machine readable. Software is used for many purposes. It can be the instruction set of hardware, in which case it is called “firmware”. It can be (part of) an operating system, an application, a library, or anything else that is executed or interpreted by a machine. In this definition, the term is to be understood in its broadest possible sense
Testing Environment	hardware, software and infrastructure necessary to evaluate (operate) the Product under Evaluation
Testing Laboratory	Accredited Conformity Assessment Body that is licensed by a Certification Body for conducting specific evaluation activities relating to the assessment of a Product under Evaluation

1.4 Abbreviations

Term	Description
3GPP	Third Generation Partnership Project
CB	Certification Body
CSA	Cyber Security Act
CVE	Common Vulnerability and Exposures
EfA	Elements for Assessment
GIAC	Global Information Assurance Certification
ICT	Information and Communications Technology
IEC	International Electrotechnical Commission

Term	Description
ISO	International Organisation for Standardization
NCCA	National Cybersecurity Certification Authority
NESAS	Network Equipment Security Assurance Scheme
NESAS CCS	NESAS Cybersecurity Certification Scheme
NP	Network Product
PuE	Product under Evaluation
SANS	SysAdmin, Audit, Network, and Security
SCAS	Security Assurance Specification
SD	Supporting Document
TL	Testing Laboratory

1.5 References

Ref	Doc Number	Title
[1]	RFC 2119	"Key words for use in RFCs to Indicate Requirement Levels", S. Bradner, March 1997. Available at http://www.ietf.org/rfc/rfc2119.txt
[2]	ISO/IEC 17025	General requirements for the competence of testing and calibration laboratories
[3]	3GPP Security Assurance Specifications	List of 3GPP-defined Security Assurance Specifications, https://www.gsma.com/security/nesas-security-assurance-specifications/

1.6 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 [1]."

2 Product Evaluation Process

Accredited NESAS Security Test Laboratories are capable of performing security evaluations of network products against the security requirements and test cases defined by 3GPP. Equipment vendors that wish to have their network products evaluated can select and contract directly with one of the recognised NESAS Security Test Laboratories listed on the scheme owner's Web Site.

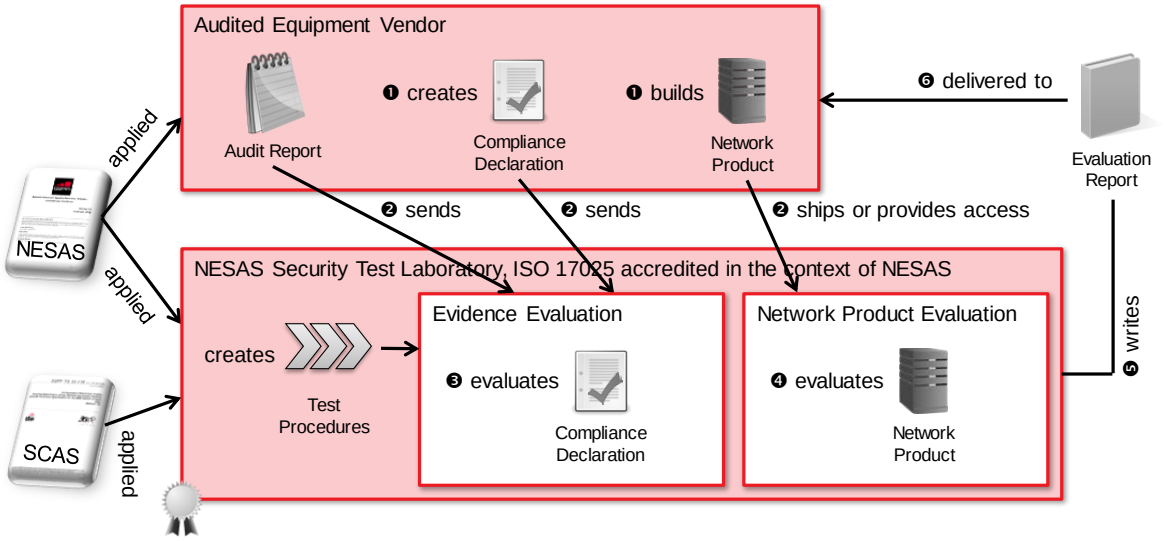

Figure 1 Evaluation of a Network Product

2.1 Evaluation Prerequisites

In order for a NESAS Network Product evaluation to be performed, the Equipment Vendor must provide the NESAS Security Test Laboratory with a number of key enablers, including the following;

- Access to the Network Product to be evaluated and all relevant documentation pertaining to its functionality, set-up, configuration, etc.
- Confirmation of the dedicated release of the Network Product to be evaluated and to the SCAS versions, contained in the SCAS List [3], under which the evaluation is to be performed as these details are to be recorded in the Evaluation Report
- Audit Report, and any related Interim Audit Reports, from the independently audited development and product lifecycle management processes
- Compliance Declaration containing Compliance Evidence from the Equipment Vendor confirming its adherence to the specific development and product lifecycle management processes that have been NESAS assessed and under which the Network Product under evaluation was developed

The NESAS Security Test Laboratory and the Equipment Vendor agree on the 3GPP defined functions supported by the Network Product under evaluation. The relevant SCAS versions against which the evaluation is to be performed are identified and agreed by both parties and this defines the scope of the evaluation.

2.2 Evaluation Preparation

In preparation for a Network Product evaluation the Equipment Vendor, shall provide to the NESAS Security Test Laboratory the following;

- Diagrammatic identification of the Network Product under evaluation and simulated systems, interfaces and protocols required to interact
- Hardware used with configuration parameters, clearly identifying which parts are running in the different hardware elements
- Operating system and version per test case

- Tools and the versions of them necessary to trigger functionalities or capture specific test evidence and results
- Simulated systems and versions of them that are necessary to perform the evaluation tests

The Equipment Vendor and the NESAS Security Test Laboratory shall agree on a test plan, aligned with the relevant SCAS documents from the SCAS list [3], that describes the following;

- Scenarios and configurations to be used, as described in the previous section
- Specific product test case to validate the version of the Network Product under evaluation
- Step by step procedure to fulfil the pre-conditions defined in the applicable SCAS
- Step by step test execution for the Network Product under evaluation necessary to conduct the tests defined in the applicable SCAS
- Step by step expected results for the Network Product under evaluation in accordance with the applicable SCAS
- Optional execution evidence and current execution results.

2.3 Evaluation Performance

Network Product evaluations may be conducted at the premises of the NESAS Security Test Laboratory but may also be conducted at other locations where the Network Product and/or the test environment necessary to perform the tests exists. This could include third party facilities, including at the Equipment Vendor premises.

NESAS recognises that Network Products under evaluation could be distributed across different locations and that tests can be executed remotely. Testing can involve the use of simulated network devices and other elements that are not under evaluation but are necessary to stimulate operations on the Network Product that is under evaluation.

Consequently, tests may be required to be executed remotely, particularly where it makes little sense to physically ship the Network Product to the NESAS Security Test Laboratory or the test environment required is too complex to be re-created in the NESAS Security Test Laboratory, or both. Remote testing can be carried out in the following ways:

1. Remote testing at the Equipment Vendor facilities
2. Remote testing at the NESAS Security Test Laboratory facilities
3. Remote testing at third party facilities.

Security and quality requirements to be fulfilled by third parties are the same as those required for the NESAS Security Test Laboratory.

In all cases, NESAS Security Test Laboratory personnel shall execute the tests, but close support from Equipment Vendor or third party technical staff may be required. The test execution and procedures must comply with ISO/IEC 17025 [2] requirements at all times.

The test location must be agreed by the Equipment Vendor and NESAS Security Test Laboratory and formally stated in written form in the contract or in a different document during the evaluation process. The test location approach (scenarios, requirements and location) must comply with the test purpose and needs to be assessed and validated by the NESAS Security Test Laboratory.

The test environment needs to be set up in a way, and that set-up needs to be documented in sufficient detail, that it can be re-built at a later time to reproduce the tests, if ever considered necessary.

2.4 Evaluation Observance

The NESAS Security Test Laboratory requires assurance that the Network Product under evaluation is the version declared by the Equipment Vendor and recorded in the evaluation report. This may be easily achieved in case of on-site testing but in the case of remote testing the NESAS Security Test Laboratory and the Equipment Vendor must agree on how to provide the necessary assurance.

The preferred approach is on-site witnessing by NESAS Security Test Laboratory evaluators. In the event that on-site witnessing is not feasible, remote witnessing would be acceptable. In this case, the witnessing will be led by the NESAS Security Test Laboratory evaluators, who can require the Equipment Vendor to provide pictures, live video streaming or facilitate live interviews with relevant Equipment Vendor staff.

A representative test will be chosen to be executed in order to verify and validate correctness of the remote test execution, test environment and verification of the Network Product under evaluation.

2.5 Evidence Evaluation

An essential component of the Network Product evaluation is to verify that the Network Product under evaluation was developed in accordance, and full compliance, with the independently audited development and product lifecycle management process. This requires the NESAS Security Test Laboratory to review the Compliance Declaration and the Compliance Evidence provided by the Equipment Vendor.

The Audit Report, and any relevant Interim Audit Report, provides guidance to the NESAS Security Test Laboratory on how the Compliance Evidence is to be evaluated. Compliance Evidence for a specific security requirement may not be available and in such a case, the Equipment Vendor provides a justifiable explanation and rationale as to why the Compliance Evidence does not exist for that particular security requirement.

2.6 Evaluation Report

At the conclusion of the evaluation, a completed Evaluation Report is provided to the Equipment Vendor, which contains the results of the security tests performed on the Network Product and the results of the evidence evaluation. A copy of the Evaluation Report is provided to the scheme owner, if the evaluated Network Product is to be listed on the scheme owner's Web Site.

The following NESAS Evaluation Report contents are suggested, as a minimum;

1. Company names and contact details of test lab and vendor
2. Full description of the product under evaluation e.g. software, hardware, interfaces, data, services and scope
3. Product name, version and description of product configuration
4. Version of GSMA document FS.47, evaluation methodology, followed
5. Details of the location(s) at which the evaluation was performed
6. Description of the test environment
7. Timeline of the evaluation activities
8. List of SCAS documents, and versions, used for the evaluation and mapping of SCAS standards to network functions within the evaluated product
9. Details of product or system component elements that may not have been tested
10. Details of product and operational documentation provided by the vendor

11. List of all test cases, test names and test results executed
12. Description of test cases executed and documentation used by evaluator to do so
13. Details of basic vulnerability testing undertaken and tools used
14. NESAS Audit Report version and list of evidence examined to assess compliance of product development process to the product under evaluation

GSMA recognises that for candidate NESAS Security Test Laboratories to obtain recognition of their competence to undertake product evaluations in the scope of their ISO/IEC 17025 accreditation the national accreditation body may require the test laboratory to perform a trial evaluation. GSMA will recognise and accept Evaluation Reports that are produced by test laboratories seeking NESAS recognition in the course of trial evaluations if all of the following criteria are met;

- Personnel, utilities and processes used during the trial evaluation were deemed adequate for the performance of NESAS product evaluations by the national accreditation body;
- The national accreditation body formally recognised the competency of the test laboratory to undertake product evaluations based on the trial evaluation;
- The personnel, utilities and processes used during the trial evaluation have not been altered or improved in any way, at the insistence of the national accreditation body, that would materially alter the evaluation outcome;
- Written notification is provided by the test laboratory to GSMA confirming the adequacy of the personnel, utilities and processes used during the evaluation trial and that these were not subsequently materially altered to achieve national accreditation body recognition.

The Evaluation Report does not expire but only applies to a specific Network Product release and SCAS version. An update of either may trigger the need for an up-to-date evaluation.

The Equipment Vendor can provide the Evaluation Report to interested stakeholders.

It is at the discretion of Evaluation Report recipients to determine from the report contents if the level of security of the evaluated Network Product is sufficient for its needs.

Annex A Document Management

A.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
1.0	Feb 2022	First version developed to describe evaluation process	GSMA ISAG	James Moran, GSMA

A.2 Licensing of NESAS Documentation

This GSMA document and its content is:

i. the exclusive property of the GSMA; and
ii. provided “as is“, without any warranties by the GSMA of any kind.

Any official government (or government appointed) body wishing to use this GSMA document or any of its content:

i. for the creation of; or
iii. as referenced in;

its own documentation regarding the same or a similar subject matter, is hereby granted a licence to the copyright in this document.

This grant is subject to and upheld, as long as the above body:

a) informs the GSMA about the use of the GSMA document prior to commencing work on;
b) provides the GSMA with the finalised, i.e. most up-to-date version of; and
c) properly references the GSMA document and any extracts thereof in;

its own documentation.

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 & questions are welcome.