Network Equipment Security Assurance Scheme - Security Test Laboratory Accreditation

Version 2.0

05 February 2021

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

Security Classification: Non-confidential

Access to and distribution of this document is restricted to the persons permitted by the security classification. This document is confidential to the Association and is subject to copyright protection. This document is to be used only for the purposes for which it has been supplied and information contained in it must not be disclosed or in any other way made available, in whole or in part, to persons other than those permitted under the security classification without the prior written approval of the Association.

Copyright Notice

Disclaimer

Antitrust Notice

The information contain herein is in full compliance with the GSM Association's antitrust compliance policy.

Table of Contents

1 Introduction

This document forms part of the documentation of the GSMA Network Equipment Security Assurance Scheme (NESAS). An overview of the scheme is available in GSMA PRD FS.13 – Network Equipment Security Assurance Scheme - Overview [5].

This document defines the requirements for NESAS Security Test Laboratories and sets the standard against which accreditation is to be assessed and awarded. It provides a high-level overview of the NESAS Security Test Laboratory accreditation process and it outlines how network product and compliance evidence evaluations are performed.

1.1 Scope

The scope of this document is the NESAS Security Test Laboratory Accreditation requirements and process and the Network Product and Compliance Evidence evaluation processes.

3GPP defines the applicable Security Assurance Specifications (SCASs) for security testing used within NESAS. The accreditation requirements defined in this document are designed to ensure that accredited NESAS Security Test Laboratories have the capabilities to perform the required tasks. The Network Product and Compliance Evidence evaluation guidance is provided to assist the Equipment Vendor and the NESAS Security Test Laboratory in the performance of those activities.

1.2 Document Maintenance

NESAS has been created and developed under the supervision of GSMA's Security Assurance Group (SECAG) comprised of representatives from mobile telecom network operators and infrastructure vendors.

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

1.3 Selection of ISO/IEC 17025 for NESAS Security Test Laboratory Accreditation

ISO/IEC 17025 [3] has been selected as the standard to be achieved by security test laboratories under NESAS, this section outlines the motivation for selecting ISO/IEC 17025.

ISO/IEC 17025 is an international standard for accrediting test laboratories. It is general and can be used to accredit any test laboratory irrespective of the product under test.

ISO/IEC 17025 is well established and there is an existing infrastructure of accreditation bodies.

The International Laboratory Accreditation Cooperation (ILAC) makes it possible for accreditation bodies to mutually recognise accreditation by and from other accreditation bodies. The accreditation bodies participating in ILAC must conform to ISO/IEC 17011 [4] to demonstrate that they are capable of accrediting test laboratories.

ISO/IEC 17025 is the single global standard used for test laboratory accreditation. SECAG, during its work, reviewed some other accreditation models and schemes for test laboratories but concluded that ISO/IEC 17025 best meets the industry's needs. The evaluation process involved SECAG engaging with a number of ILAC member national accreditation bodies that provided invaluable advice on ISO/IEC 17025 and its applicability to mobile network security assurance.

The goal of ISO/IEC 17025 accreditation is to ensure worldwide comparable accuracy and correctness of output created by a NESAS Security Test Laboratory and created for a defined purpose. This ensures that operators, vendors, regulators, and any other stakeholders can trust evaluation reports created by an ISO/IEC 17025 accredited test laboratory.

ISO/IEC 17025 provides for the independence and impartiality of test laboratories. Any test laboratory that is ISO/IEC 17025 accredited in the context of NESAS is eligible to be recognised as a NESAS Security Test Laboratory under the scheme.

2   Definitions

2.1   Common Abbreviations

Term	Description
3GPP	Third Generation Partnership Project
ILAC	International Laboratory Accreditation Cooperation
NESAS	Network Equipment Security Assurance Scheme
SCAS	Security Assurance Specification
SECAG	Security Assurance Group

2.2   Glossary

Term [1]	Description
Asset	An asset is any tangible or intangible thing or characteristic that has value to an organisation. There are many types of assets. Some of these include obvious things like machines, facilities, patents, and software. But the term can also include less obvious things like services, information, and people, and characteristics like reputation and image or skill and knowledge.
Audit Report	Document presenting the results of the audit conducted at the Equipment Vendor by the Auditor
Compliance Declaration	A written statement by the Equipment Vendor that confirms it adheres to the previously assessed development and lifecycle processes for the particular Network Product that is provided to a NESAS Security Test Laboratory for evaluation.
Compliance Evidence	Evidence to be provided by the Equipment Vendor to the NESAS Security Test Laboratory, demonstrating that the Equipment Vendor applied its previously

---

[1] Unless otherwise defined, all capitalised terms shall have the same meaning as in FS13

Term [1]	Description
	internally assessed and independently audited development and lifecycle processes to build the Network Product under evaluation. All Compliance Evidence for one Network Product is collected in one Compliance Declaration.
Equipment Vendor	Organisation that develops, maintains and supplies to network operators network equipment that supports functions defined by 3GPP.
Evaluation Report	Documented assessment produced by a NESAS Security Test Laboratory of the level of compliance of a network product with the relevant 3GPP defined Security Assurance Specification
Interim Audit Report	Document presenting the results of an Interim Audit conducted at the Equipment Vendor by the Auditor that is published as an addendum to an existing Audit Report.
ISO/IEC 17025 Accreditation Body	An ILAC member that is recognised as having competence to carry out ISO/IEC 17025 test laboratory audits
NESAS Security Test Laboratory	A test laboratory that is ISO/IEC 17025 accredited in the context of NESAS and that conducts NESAS 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 Evaluation	An assessment, carried out by a NESAS Security Test Laboratory, of network products against the relevant 3GPP defined Security Assurance Specification(s)
Security Assurance Group (SECAG)	A subgroup of the GSMA Fraud and Security Group
Security Assurance Specification	Specification written by the 3GPP, containing security requirements and test cases for a dedicated 3GPP-defined Network Function or a group of Network Functions.
Test Laboratory Accreditation	The process by which a security test laboratory is assessed by a qualified ISO/IEC 17025 accreditation body to assess and accredit its level of competence

2.3   References

Ref	Title
[1]	"Key words for use in RFCs to Indicate Requirement Levels", S. Bradner, March 1997. Available at http://www.ietf.org/rfc/rfc2119.txt
[2]	"Security assurance scheme for 3GPP network products for 3GPP network product classes", TS 33.916, defined by 3GPP SA3 Available at http://www.3gpp.org/DynaReport/33916.htm
[3]	"General requirements for the competence of testing and calibration laboratories", ISO/IEC 17025, 2005
[4]	"Conformity assessment -- General requirements for accreditation bodies accrediting conformity assessment bodies", ISO/IEC 17011, 2004
[5]	FS.13 – Network Equipment Security Assurance Scheme - Overview

Ref	Title
[6]	NESAS Web Site at https://gsma.com/nesas
[7]	SCAS list at https://www.gsma.com/security/nesas-security-assurance-specifications/

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 [1]."

3 Definition of NESAS Security Test Laboratory

A Security Test Laboratory in the context of NESAS is a security test laboratory that evaluates a network product according to one or several 3GPP SCASs and the security requirements defined in Section 7 below.

In addition, this Security Test Laboratory evaluates the Compliance Evidence provided by the Equipment Vendor that the Network Product under evaluation was developed in adherence to the previously assessed vendor development and lifecycle processes.

This document defines the requirements for how a security test laboratory can become accredited in accordance with NESAS. It also provides guidance on the performance of Network Product and Compliance Evidence evaluations.

Further details on the role of the Security Test Laboratory and its tasks are described in the NESAS Overview document FS.13 [5].

4 Security Objectives

The accredited entity is responsible for ensuring that assets are protected from the risks to which they are exposed. It is this protection that provides assurance to the mobile network operators. A range of security objectives must be addressed but higher levels of assurance are needed depending on the asset classification.

The overall objective is to maintain the existence and integrity of the assets.

The desire of the mobile industry is to ensure that security test laboratories are set up and maintained that are capable of performing meaningful, comprehensible, repeatable, and complete tests of network equipment. NESAS Security Test Laboratories must ensure they reach and maintain the standard described in this document.

5 Security Test Laboratory Assets

The main assets of a security test laboratory that need to be protected are:

- Competence of the laboratory personnel
- Working processes and guidelines for the laboratory
- Equipment and tools available to and used by the laboratory.

6 Security Test Laboratory Threats

Threats related to the security test laboratory assets and to which they are exposed are:

- The laboratory personnel are not sufficiently competent
- The laboratory lacks suitable working procedures and guidelines
- The laboratory lacks suitable equipment and tools.

7 Security Test Laboratory Requirements

In order to have sufficient confidence in a security test laboratory's competence and capabilities, certain requirements must be met. The overriding requirement is to achieve ISO/IEC 17025 [3] accreditation, which encompasses a range of requirements that must be satisfied.

The Security Test Laboratory must be specifically ISO/IEC 17025 accredited to

- perform tests as defined in the 3GPP SCASs within the NESAS scope and to

- perform Compliance Evidence evaluations as defined by NESAS.

To be recognised as a competent authority with the requisite expertise, capabilities, equipment, procedures, and environment. GSMA has defined guidelines for test laboratories and ILAC member accreditation bodies on what is expected of candidate NESAS security test laboratories to demonstrate their competency and have NESAS included in the scope of their ISO/IEC 17025 accreditation. Full details are available in Annex A below.

NESAS requires, that the defined period for which reports and relevant records as defined in section 8.4 in ISO/IEC 17025 must be retained is the lifetime of the Network Product.

8 Accreditation Process

The NESAS Security Test Laboratory accreditation process exists to formally recognise that a test laboratory is impartial and competent to evaluate a 3GPP network product against the security requirements defined by 3GPP in its SCAS documents and to produce an Evaluation Report.

The first step to achieve accreditation, and to be recognised as a test laboratory capable of evaluating product compliance against security requirements, is for a security test laboratory to contact a recognised ILAC member ISO/IEC 17025 accreditation body with a request to be ISO/IEC 17025 audited and accredited. The ISO/IEC 17025 accreditation body will follow the processes applicable to the ISO/IEC 17025 accreditation standard to assess the competence of the security test laboratory.

In addition to the requirements defined in the ISO/IEC 17025 standard, GSMA reserves the right to define additional security requirements that need to be fulfilled as part of the NESAS Security Test Laboratory Accreditation process. The ISO/IEC 17025 accreditation body must be provided with a copy of the current version of this document and the NESAS Security Test Laboratory Competency Guidelines contained in Annex A below, to ensure it

understands what security requirements are applicable at the time the accreditation is sought.

NESAS fully recognises the competency of ILAC member accreditation bodies to assess and accredit security test laboratories. Therefore, all security test laboratories that are deemed by an ILAC member to have satisfied the ISO/IEC 17025 and NESAS requirements, and that have been ISO/IEC 17025 accredited, will be considered to have achieved NESAS accreditation.

After ISO/IEC 17025 accreditation has been achieved the successful security test laboratory will inform the GSMA and provide a copy of its ISO/IEC 17025 certificate, referencing NESAS. The laboratory's details (incuding validity dates) will be recorded and published on the GSMA's NESAS Web Site **Error! Reference source not found.**. It is the responsibility of the NESAS Security Test Laboratory to keep its ISO/IEC 17025 accreditation current. Failure to do so will cause its recognition of its competency to conduct network product evaluations to lapse and become invalid.

9   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 by GSMA on its Web Site **Error! Reference source not found.**.
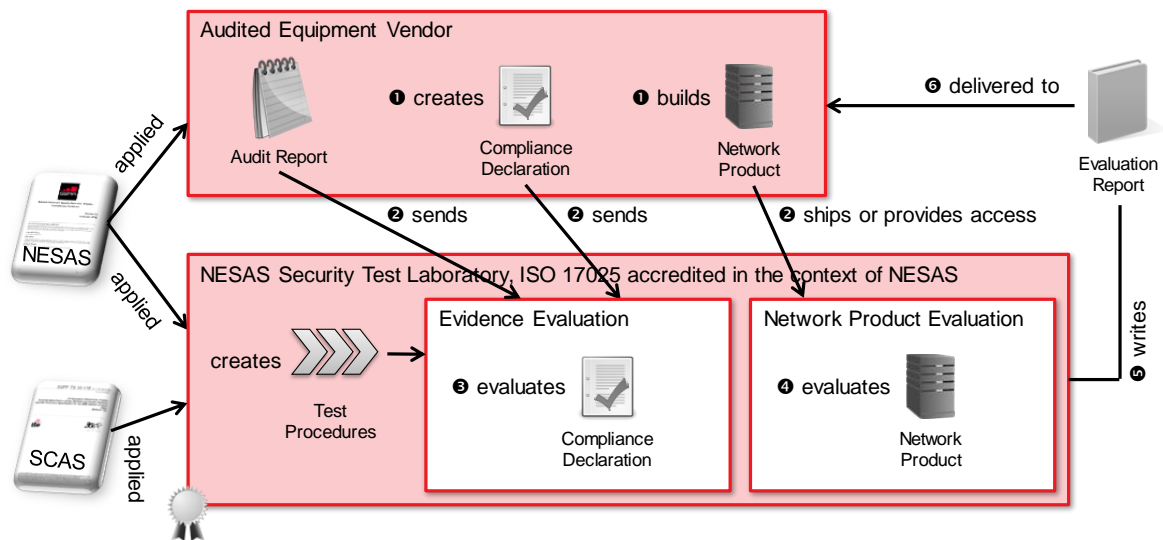

Figure 1 Evaluation of a Network Product

9.1   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 **Error! Reference source not found.**, 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 Conformance 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.

9.2   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 **Error! Reference source not found.**, 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.

9.3   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 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.

9.4   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.

9.5   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.

9.6   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 GSMA, if the evaluated Network Product is to be listed on the NESAS Web Site **Error! Reference source not found.**.

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   NESAS Security Test Laboratory Competency Guideline Requirements

A.1   Introduction

One of the requirements defined under GSMA's Network Equipment Security Assurance Scheme (NESAS) [1] is that NESAS Security Test Laboratories are accredited to ISO/IEC 17025. As part of that accreditation, the NESAS Security Test laboratory must demonstrate its competencies to undertake NESAS product evaluations against the security requirements defined by 3GPP in its Security Assurance Specification (SCAS) [2] documents.

This document describes the experience and skills that Evaluators in the NESAS Security Test Laboratory must have to execute their role effectively in order to meet the requirements of GSMA NESAS.

A.1.1   Purpose

The document is primarily intended to guide organisations that;

   I.   Apply to be recognised NESAS Security Test Laboratories that operate under the GSMA NESAS rules or

   II.   Act as ISO/IEC 17025 accreditation bodies for NESAS Security Test laboratories.

A.1.2   Glossary

Term	Description
Audit Report	Document presenting the results of the audit conducted at the Equipment Vendor by the Auditor.
Interim Audit Report	Document presenting the results of an interim audit conducted at the Equipment Vendor by the Auditor that is published as an addendum to an existing Audit Report.
Auditor	Individual that is qualified to perform Vendor Development and Product Lifecycle Processes audits and makes up part of the Audit Team.
Compliance Declaration	A written statement by the Equipment Vendor that confirms it adheres to the previously assessed development and lifecycle processes for the particular Network Product that is provided to a NESAS Security Test Laboratory for evaluation.
Compliance Evidence	Evidence to be provided by the Equipment Vendor to the NESAS Security Test Laboratory, demonstrating that the Equipment Vendor applied its previously internally assessed and independently audited development and lifecycle processes to build the Network Product under evaluation. All Compliance Evidence for one Network Product is collected in one Compliance Declaration.
Evaluation Report	Documented assessment produced by a NESAS Security Test Laboratory of the level of compliance of a network product with the relevant 3GPP defined Security Assurance Specification and also the result of the evaluation of Compliance Evidence provided by vendor on whether network products are developed according to audited process.

| Term	Description
Evaluation Team	The Evaluators from a NESAS Security Test Laboratory that are assigned to evaluate a vendor's network product.
Evaluator	A member of the NESAS Security Test Laboratory organisation that conducts NESAS network product evaluations.
ISO/IEC 17025 Accreditation Body	An ILAC member that is recognised as having competence to carry out ISO/IEC 17025 test laboratory audits.
NESAS Security Test Laboratory	A test laboratory that is ISO/IEC 17025 accredited in the context of NESAS and that conducts network product evaluations.

A.2   Overview

The process for awarding GSMA NESAS Security Test Laboratory Accreditation is designed to ensure that the candidate Test Laboratory has sufficiently demonstrated that it is technically competent in the specific field of ICT security evaluation under GSMA NESAS.

The NESAS process includes the need for the Test Laboratory to demonstrate that it, and specifically the Evaluators assigned by the laboratory, have the ability

> i.   to execute the test cases defined in the 3GPP Security Assurance Specifications (SCAS) [2]; and
> ii.   to evaluate Compliance Evidence that the vendor, whose product is being evaluated, has complied with the development and product lifecycle processes that were assessed and audited by the GSMA NESAS auditors.

A.3   Evaluator/Evaluation Team Competency

The requirements provided below act as supplementary competency requirements to the requirements contained in ISO/IEC 17025 and within NESAS. They are intended to be helpful to experts collaborating and supporting the ISO/IEC 17025 accreditation body (so-called subject matter experts). As such, these guidelines are intended to assist the "subject matter expert" to ensure high quality SCAS evaluations, can be executed by an Evaluator/Evaluation Team, as the SCAS standards are new to the industry as described in FS.13 'NESAS Overview' (which can be obtained at [1]) and as depicted below.
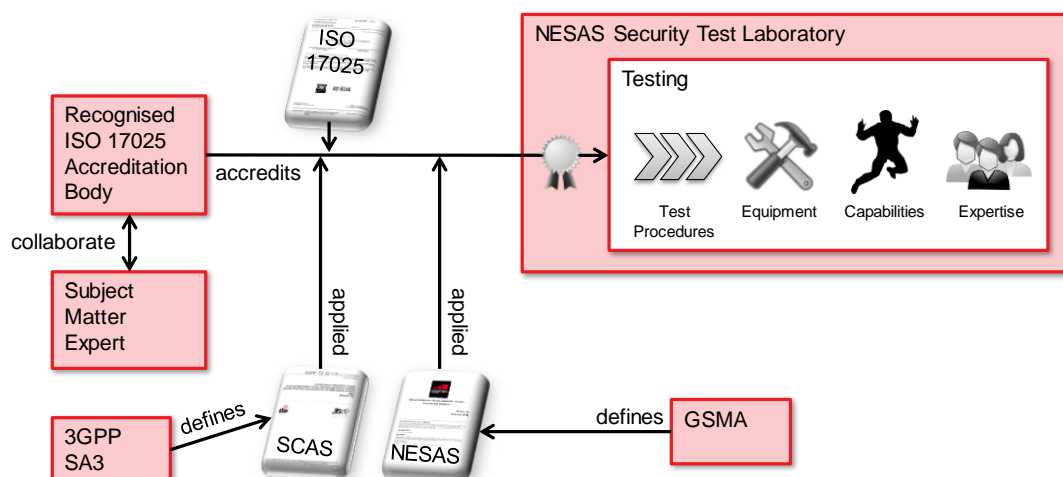
Evaluators will need to demonstrate relevant knowledge of the tasks they are assigned. The Evaluation Team working within the definition of NESAS is required to:

- Understand the principles and methods used in NESAS,

- Understand the relationship between the 3GPP Security Assurance Specification documents and other NESAS documents used by the scheme,

- Demonstrate an understanding of the overall evaluation planning process (i.e. how to interpret the Audit Report/Interim Audit Report, what to look for in terms of Compliance Evidence evaluation, how to plan and execute the relevant SCAS test cases on vendor products, etc.,

- Be able to analyse the results of the SCAS testing including vulnerability scans according to the relevant SCAS test cases,

- Be able to evaluate Compliance Evidence (provided by the vendor for the product under evaluation) that the product was developed according to the audited process. The NESAS vendor development and product lifecycle process Audit Report, and Interim Audit Report if applicable, indicates the type of evidence that should be provided to the Evaluators to facilitate the 'evidence evaluation' task,

- Be able to independently document the evaluation results of his or her work objectively, precisely, correctly, unambiguously, and at the level of detail required by NESAS (namely to create NESAS Evaluation reports to the level of detail specified in the ISO/IEC 17025 standard). The NESAS Evaluation Report must ensure that the level of detail allows for reproducibility of the tests results,

- The Evaluation Team should clearly demonstrate its understanding of the SCAS evaluation methodology and process including:

  o How SCAS requirements are defined,

- o How to select the relevant SCAS documents from the SCAS list **Error! Reference source not found.** in order to test a specific network equipment product,

  - o What are the inputs to a SCAS evaluation,

  - o What is the meaning of the SCAS evaluation to the operator.

- The Evaluation Team is expected to be familiar with telecom equipment and network related knowledge, such as security architecture, interfaces, protocols, interaction procedures and messages, typical attack surfaces, attack patterns and vulnerabilities.

In addition to the general competency requirements described in this section, the Evaluation Team shall have sufficient technical competence for the tasks it performs. It is the NESAS Security Test Laboratory's responsibility to determine the competencies needed within the NESAS Evaluation Team for each evaluation, to appoint Evaluators accordingly, and, if necessary, to augment the Evaluation Team with internal or external technical experts.

Although not especially specified in NESAS, it is expected that:

- Evaluators appointed to the Evaluation Team have relevant knowledge, working experience and/or education in order to fulfil the needs to be a NESAS Security Test Laboratory Evaluator.

- The Evaluation Team has a team leader who is highly experienced to supervise, oversee and monitor the activities of less experienced Evaluators and the additional specialists and technical experts.

Guidance for identifying relevant knowledge, experience, skills or educational qualifications could be:

- Several years (2-3+) experience working on ICT security testing (security functional testing, penetration testing, ethical hacking, or related fields),

- External security testing qualifications (such as Certified Ethical Hacker, SANS Ethical hacker certification, GIAC certifications).

A.4   Testing Equipment and Tools

A NESAS Security Test Laboratory should have access to testing equipment and tools for 3GPP SCAS testing such as fuzz testing tools and scanning tools, which are commercial tools or commonly used.

References

1. GSMA NESAS documents

https://www.gsma.com/security/network-equipment-security-assurance-scheme/

2. 3GPP Security Assurance Specifications

https://www.gsma.com/security/nesas-security-assurance-specifications/

Abbreviations

3GPP   Third Generation Partnership Project

GIAC   Global Information Assurance Certification

ICT   Information and Communications Technology

ILAC   International Laboratory Accreditation Cooperation

ISO   International Organisation for Standardization

NESAS   Network Equipment Security Assurance Scheme

SCAS   Security Assurance Specification

Annex B   Document Management

B.1   Document History

Version	Date	Brief Description of Change	Editor / Company
1.0	Aug 2019	Release 1 approved by SECAG	James Moran, GSMA
1.1	Aug 2020	Addition of test lab competency guidelines	James Moran, GSMA
2.0	Feb 2021	Definition of 'Compliance Evidence' added Evidence evaluation added to test lab reqs Dispute resolution process removed NESAS Oversight Board removed Auditor definition updated References to GSMA NESAS web site added New section added on product evaluation extending the scope of the document	James Moran, GSMA

B.2   Document and NESAS Release Mapping History

Document Version	Applicable NESAS Release
1.0	NESAS 1.0
1.1	NESAS 1.1
2.0	NESAS 2.0

B.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 always welcome.