Network Equipment Security Assurance Scheme - Security Test Laboratory Accreditation

Version 2.3

15 September 2023

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 forms part of the documentation of the Network Equipment Security Assurance Scheme (NESAS). An overview of the scheme is available in GSMA PRD FS.13 – Network Equipment Security Assurance Scheme - Overview[4].

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 and authorisation process.

1.1 Scope

The scope of this document is the NESAS Security Test Laboratory Accreditation and authorisation requirements and process.

3GPP, or other recognised standards development organisations, define the applicable Security Assurance Specifications (SCASs) in accordance with guidelines defined by NESAS Group in FS.50 [7] for security testing that can be adopted by NESAS Group for use within NESAS in accordance with the process defined in FS.47 [6]. The accreditation requirements defined in this document are designed to ensure that accredited and authorised NESAS Security Test Laboratories have the capabilities to perform the required tasks.

1.2 Document Maintenance

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 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.

1.3 Definitions

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 Vendor Development and Product Lifecycle Processes for

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

Term [1]	Description
	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 Vendor Development and Product Lifecycle Processes to build the Network Product under evaluation. All Compliance Evidence for one Network Product is collected in one Compliance Declaration. Note: An Auditor defines in the Audit Report, which Compliance Evidence is required for subsequent product evaluations.
Equipment Vendor	Organisation that develops, maintains and supplies network equipment that supports functions defined by 3GPP.
Evaluation Report	Documentation of the results of Evidence Evaluation and Network Product Evaluation, produced by an accredited NESAS Security Test Laboratory.
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 Group	The Industry Specification Issuing Group (ISIG) of the GSMA (see GSMA PRD AA.35 [5] for details) that is tasked with the overall implementation, governance, maintenance and further development of NESAS specifications.
NESAS Security Test Laboratory	A test laboratory that is ISO/IEC 17025 accredited in the context of NESAS and that is authorised to conduct NESAS Network Product evaluations.
Network Product	Network Equipment developed, maintained and supplied by an Equipment Vendor, consisting of one or more Network Function(s).
Network Product Evaluation	Activity of evaluating the Product under Evaluation (PuE) in NESAS, according to requirements and test cases taken from NESAS-adopted Security Assurance Specifications (SCAS).
Scheme Owner	Organisation or authority responsible for developing and maintaining a specific security assurance or certification scheme that uses the NESAS specifications (refer to Annex **Error! Reference source not found.** for licensing of NESAS Documentation).
Security Assurance Specification	Specification containing security requirements and test cases for a defined Network Function or a group of Network Functions. It is created and maintained by a Standards Development Organisation (SDO).
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

1.4 Abbreviations

Term	Description
3GPP	Third Generation Partnership Project
ILAC	International Laboratory Accreditation Cooperation

Term	Description
NESAS	Network Equipment Security Assurance Scheme
PRD	Permanent Reference Document
SCAS	Security Assurance Specification

1.5 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]	"General requirements for the competence of testing and calibration laboratories", ISO/IEC 17025, 2005
[3]	"Conformity assessment -- General requirements for accreditation bodies accrediting conformity assessment bodies", ISO/IEC 17011, 2004
[4]	GSMA PRD FS.13 – Network Equipment Security Assurance Scheme - Overview
[5]	GSMA PRD AA.35 – Procedures for Industry Specifications
[6]	GSMA PRD FS.47 – NESAS - Product and Evidence Evaluation Methodology
[7]	GSMA PRD FS.50 - Network Equipment Security Assurance Scheme – Security Assurance Specification Development Guidelines
[8]	SCAS list at https://www.gsma.com/security/nesas-security-assurance-specifications/
[9]	NESAS Web Site https://gsma.com/nesas

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

ISO/IEC 17025 [2] 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 [2].

ISO/IEC 17025 [2] 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 [2] 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 [3] to demonstrate that they are capable of accrediting test laboratories.

ISO/IEC 17025 [2] is the single global standard used for test laboratory accreditation.

The goal of ISO/IEC 17025 [2] 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 [2] accredited test laboratory.

ISO/IEC 17025 [2] 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 and authorised as a NESAS Security Test Laboratory under the scheme.

3 Definition of NESAS Security Test Laboratory

A Security Test Laboratory in the context of NESAS is a security test laboratory that is authorised to evaluate 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 and authorised in accordance with NESAS.

Network Product evaluations can only be performed by test laboratories that are independent of the Equipment Vendors that develop and maintain Network Products under evaluation.

Further details on the role of the Security Test Laboratory and its tasks are described in the NESAS Overview document FS.13 [4].

4 Security Objectives

The accredited and authorised 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 and other industry stakeholders. 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 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 of test laboratory assets and to which they are exposed include:

- 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 [2] 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 and authorised as a competent authority, test laboratories must have and demonstrate the requisite expertise, capabilities, equipment, procedures, and environment. The NESAS Group 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 a period of at least ten (10) years after the Evaluation Report has been issued by the NESAS Security Test Laboratory.

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, additional security requirements that need to be fulfilled as part of the NESAS Security Test Laboratory

Accreditation process may be adopted. 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 and will be eligible to be authorised to perform NESAS Network Product Evaluations.

After ISO/IEC 17025 accreditation has been achieved the successful security test laboratory will inform the Scheme Owner and provide a copy of its ISO/IEC 17025 certificate, referencing NESAS. The laboratory's details (including validity dates) will be recorded and published on the Scheme Owner's NESAS Web Site [9]. 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 and authorisation to conduct network product evaluations to lapse and become invalid.

Annex A NESAS Security Test Laboratory Competency Guideline Requirements

A.1 Introduction

One of the requirements defined under the Network Equipment Security Assurance Scheme (NESAS) is that NESAS Security Test Laboratories are accredited to ISO/IEC 17025 [2]. 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 in Security Assurance Specification (SCAS) [8] 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 NESAS.

A.1.1 Purpose

The document is primarily intended to guide organisations that:

I. Apply to be accredited NESAS Security Test Laboratories that operate under the 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 Audit Team.
Interim Audit Report	Document presenting the results of an interim audit conducted at the Equipment Vendor by the Audit Team 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. Note: This definition does not mandate a certain employer for the Auditor, which is possibly employed by a dedicated Auditing Organisation (or could be freelancer). The qualification is ensured by the certification of said individuals.
Compliance Declaration	A written statement by the Equipment Vendor that confirms it adheres to the previously assessed Vendor 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 Vendor Development and Product Lifecycle Processes to build the Product under evaluation. All Compliance Evidence for one Network Product is collected in one Compliance Declaration. Note: An Auditor defines in the Audit Report, which Compliance Evidence is required for subsequent product evaluations.
Evaluation Report	Documentation of the results of Evidence Evaluation and Network Product Evaluation, produced by an accredited NESAS Security Test Laboratory.

Term	Description
Evaluation Team	The Evaluators from a NESAS Security Test Laboratory that are assigned to evaluate an Equipment 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 [2] test laboratory audits.
NESAS Security Test Laboratory	A test laboratory that is ISO/IEC 17025 accredited in the context of NESAS and that is authorised to conduct Network Product evaluations.

A.2 Overview

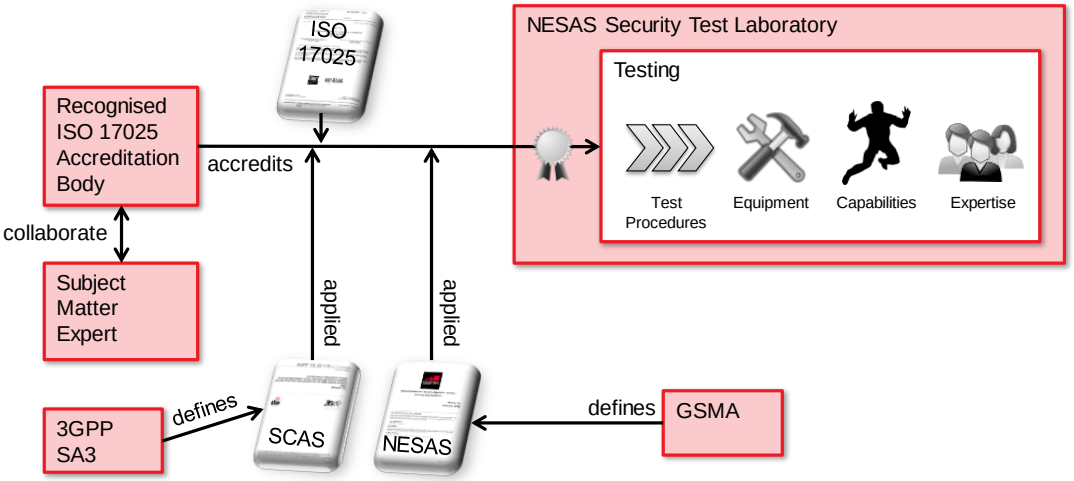
The process for awarding NESAS Security Test Laboratory Accreditation is designed to ensure that the candidate Test Laboratory has sufficiently demonstrated that it is technically competent in the specific field of ICT security evaluation under NESAS.

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 Security Assurance Specifications (SCAS) [8]; 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 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 [2] and within NESAS. They are intended to be helpful to experts collaborating and supporting the ISO/IEC 17025 [2] 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.



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 competent in using relevant testing tools (see Section **Error! Reference source not found.**), how to configure them, how to apply them, how to interpret their results. Evaluators understand how the tools work and are able to apply them in an effective way so that their results actually represent a statement on the Network Product's security,
- 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 [2] 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:
    - How SCAS requirements are defined,
    - How to select the relevant SCAS documents from the SCAS list [8]in order to test a specific network product,
    - What are the inputs to a SCAS evaluation,
    - What is the meaning of the SCAS evaluation to the mobile network 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 SCAS testing such as fuzz testing tools, vulnerability and port scanning tools and configuration checking tools, which are Commercial-off-the-Shelf (COTS) and Free-Open-Source-Software (FOSS) tools.

Some of the tools may require configuration prior to testing, in order to get meaningful results. For example, it may be necessary to provide the tool with login credentials or a file system path to a configuration file of the tested network service. The Evaluation Team shall have necessary detailed knowledge about the tools it uses, to apply them adequately.

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 NESAS Group	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 NESAS web site added New section added on product evaluation extending the scope of the document	James Moran, GSMA
2.1	Jan 2022	Product evaluation section removed and specific references to GSMA removed to ensure the document is more widely applicable to schemes derived from NESAS. A statement on NESAS documentation licensing has also been added.	James Moran, GSMA
2.2	Oct 2022	Changes made to facilitate the introduction of fees and contract changes to place NESAS on a sustainable financial footing.	James Moran, GSMA
2.3	Sep 2023	Definitions updated to align with other scheme documents and updates made pertaining to 'scheme owner'. References to defunct TR 33.916 removed Clarification added that product evaluations must be performed by independent test labs Test lab record retention requirement updated References added to SCAS development guidelines and GSMA adoption process Competency requirement on testing tools added	James Moran, GSMA

B.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
ii. 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.

B3 Other Information

Type	Description
Document Owner	GSMA NESASG
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.