Network Equipment Security Assurance Scheme - Security Test Laboratory Accreditation

Version 1.1

27 July 2020

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

Security Classification: Non-confidential

Copyright Notice

Disclaimer

Antitrust Notice

Table of Contents

1 Introduction

This document 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 also provides a high level overview of the NESAS Security Test Laboratory accreditation process.

1.1 Scope

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

It is 3GPP that 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.

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. AnyTest 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.
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
ISO/IEC 17025 Accreditation Body	An ILAC member that is recognised as having competence to carry out ISO/IEC 17025 test laboratory audits
NESAS Oversight Board	The body overseeing NESAS, run by the GSMA. It is responsible for the governance of the Vendor Development and Product Lifecycle Process assessments and audits.
NESAS Security Test Laboratory	A test laboratory that conducts NESAS network product evaluations
Network Product	Network equipment produced and sold to network operators by an Equipment Vendor

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

Term [1]	Description
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
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

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.

This document defines the requirements for how a security test laboratory can become accredited in accordance with NESAS.

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 Requirements

In order to have sufficient confidence in a security test laboratory's competence and capabilities, certain security requirements must be met. The overriding security 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 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 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 website. 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 NESAS Dispute Resolution Process

The NESAS Dispute Resolution Process is described in section 3.6 of FS.13 [5].

9.1 Possible Dispute Scenarios

The following table illustrates a number of possible dispute scenarios that could arise within the Security Test Laboratory accreditation element of NESAS that involve a variety of parties. The table merely captures example scenarios and is not intended to be exhaustive.

	Operator	Vendor	Test Lab	NESAS OB
Operator		NP or development and lifecycle process security inconsistency		Operator believes SCAS is inadequate or challenges auditor accreditation
Vendor	NP or development and lifecycle process security inconsistency		Third party test lab refuses product evaluation	SCAS documentation ambiguous or not fit for purpose
Test Lab		Third party test lab refuses product evaluation		SCAS documentation ambiguous or not fit for purpose
NESAS Oversight Board (OB)	Operator believes SCAS is inadequate or challenges auditor findings	SCAS documentation ambiguous or not fit for purpose	SCAS documentation ambiguous or not fit for purpose	

Table 1 Example Dispute Scenarios

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.
Auditor	Organisation appointed and contracted by GSMA and selected by Equipment Vendor to conduct audits of Vendor Development and Product Lifecycle Processes.
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 evidence provided by vendor on whether network products are developed according to audited process.
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

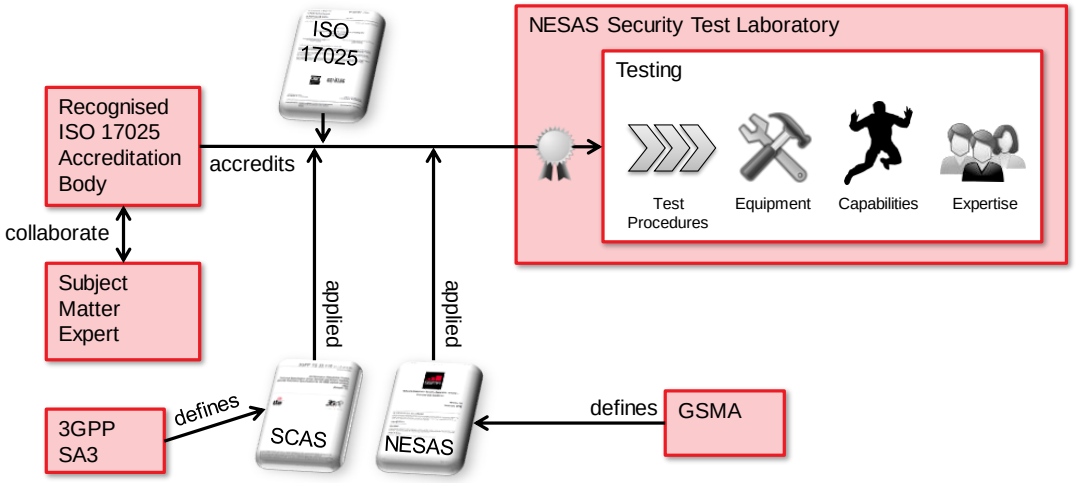
The process for awarding GSMA NESAS Security Test Laboratory Accreditation is designed to ensure that the candidate Test Laboratory has sufficiently demonstrated that it is technically competent in the specific field of ICT security evaluation under GSMA NESAS.

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 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, what to look for in terms of 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 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 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:
    - How SCAS requirements are defined,
    - How to select the relevant SCAS documents in order to test a specific network equipment product,
    - What are the inputs to a SCAS evaluation,
    - 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

B.2 Document and NESAS Release Mapping History

Document Version	Applicable NESAS Release
1.0	NESAS 1.0
1.1	NESAS 1.1

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.