Network Equipment Security Assurance Scheme - Security Test Laboratory Accreditation

Version 1.0

07 October 2019

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 suppliers.

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

1.3 Selection of ISO 17025 for NESAS Security Test Laboratory Accreditation

ISO 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 17025.

ISO 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 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 recognize accreditation by and from other accreditation bodies. The accreditation bodies participating in ILAC must conform to ISO 17011 [4] to demonstrate that they are capable of accrediting test laboratories.

ISO 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 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 17025 and its applicability to mobile network security assurance.

The goal of ISO 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 17025 accredited test laboratory.

ISO 17025 provides for the independence and impartiality of test laboratories. Any NESAS Security Test Laboratory that is ISO 17025 certified is permissible 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 organization. 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 17025 Accreditation Body	An ILAC member that is recognised as having competence to carry out ISO 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 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 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 17025, 2005
[4]	"Conformity assessment -- General requirements for accreditation bodies accrediting conformity assessment bodies", ISO 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 17025 [3] accreditation, which encompasses a range of requirements that must be satisfied.

The Security Test Laboratory must be specifically ISO 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.

NESAS requires, that the defined period for which reports and relevant records as defined in section 4.13.2.1 in ISO 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 17025 accreditation body with a request to be ISO 17025 audited and accredited. The ISO 17025 accreditation body will follow the processes applicable to the ISO 17025 accreditation standard to assess the competence of the security test laboratory.

In addition to the requirements defined in the ISO 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 17025 accreditation body must be provided with a copy of the current version of this document 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 17025 and NESAS requirements, and that have been ISO 17025 accredited, will be considered to have achieved NESAS accreditation.

After ISO 17025 accreditation has been achieved the successful security test laboratory will inform the GSMA and provide a copy of its ISO 17025 certificate. 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 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 Document Management

A.1 Document History

Version	Date	Brief Description of Change	Editor / Company
1.0	Aug 2019	Release 1 approved by SECAG	James Moran, GSMA

A.2 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.