FS.14 Network Equipment Security Assurance Scheme – Security Test Laboratory Accreditation

Version 0.7
March 2016

Security Classification: Non-confidential

Copyright Notice

Disclaimer

Antitrust Notice

Table of Contents

1 Introduction

This document is part of the GSMA Network Equipment Security Assurance Scheme (NESAS), of which there is an overview available in FS.13 – NESAS 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 the document has been restricted only to matters pertaining to the NESAS Security Test Laboratory Accreditation requirements and process.

Consistency of the accreditation requirements has been achieved by defining:

- NESAS Security Test Laboratory
- Security objectives to be achieved
- Assets to be protected
- Risk and threats mapped against the objectives
- Accreditation requirements

3GPP defines Security Assurance Specifications (SCASs) for security testing within the 3GPP defined Security Assurance Methodology (SECAM) [2]. The accreditation requirements defined in this document are designed to ensure the NESAS security test laboratories which have been accredited against the accreditation requirements have the capabilities to perform the tasks defined within SECAM.

1.2 Document Maintenance

This standard 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 GSM Association is responsible for maintaining this security standard and for facilitating a review, involving all relevant stakeholders, which will take place every 12 months during the life of the scheme.

1.3 Motivation for Selection of ISO 17025 for NESAS Security Test Laboratory Accreditation

ISO 17025 has been selected as the standard to be achieved by competent security test laboratories and this section outlines the motivation for selecting that particular standard.

ISO 17025 is an international standard for accrediting test laboratories. It is general and can thus be used to accredit any test laboratory, irrespective of what kind of product a test laboratory is performing tests on.

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.

In practice, 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 testing lab and created for a defined purpose. This ensures that operators, vendors, regulators, and any other possibly relevant parties can trust evaluation reports created by an ISO 17025 accredited lab.

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
SECAM	Security Assurance Methodology
SECAG	Security Assurance Group

2.2 Glossary

Term	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.
Commercially Relevant Lifetime	Commercially relevant is the time during which the Network Product it operated in a production network and maintenance by the supplier is required by means of commercial agreements or regulatory stipulations.
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	An ILAC member that is recognised as having competence to carry out ISO 17025 test laboratory audits

Term	Description
Body	
NESAS Accreditation Board	Responsible for developing requirements on vendor network product development, network product lifecycle management process, and NESAS accreditation of vendors and NESAS security test laboratories
NESAS Security Test Laboratory	A vendor owned or third party owned test laboratory that conducts network product evaluations
Network Product	Network equipment produced and sold to network operators by an Equipment Vendor
Network Product Evaluation	An assessment, carried out by a security test lab, of network products against the relevant 3GPP defined Security Assurance Specification
Security Assurance Group	A subgroup of the GSMA Fraud and Security Group
Standard	The requirements defined in this document that must be satisfied by a security test laboratory to achieve accreditation
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 vendor owned security test laboratory or a third party owned security test laboratory that evaluates a network product according to one or several 3GPP SCASs.

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 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. Security test laboratories must ensure they reach and maintain the standard described in this document.

5 Assets

Within the definition oben, certain assets are sensitive and their integrity must be protected.

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

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

6 Threats

6.1 Introduction

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

- The laboratory personnel is 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, which is outlined below, is to achieve ISO 17025 accreditation, which encompasses a range of requirements that must be satisfied. This is considered fundamental and the minimum required.

The security test laboratory shall be accredited according to ISO 17025 [3] in order for it to be recognised as a competent authority having the skills and tools to be able to perform tests according to 3GPP SCASs and according to the scope of NESAS.

NESAS requires, that the defined period for which reports and relevant records as defined in 4.13.2.1 in ISO 17025 must be retained is for the Commercially Relevant 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, additional security requirements that may be defined by NESAS and included in Section 7 of this document need to be fulfilled as part of the security test laboratory accreditation process. The ISO 17025 accreditation body will 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 and, by extension, what it needs to assess to satisfy the NESAS requirements.

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 NESAS Accreditation Board and provide a copy of its ISO 17025 certificate. The NESAS Accreditation Board will recognise the outcome and accredit the test laboratory. The security test laboratory’s details will be recorded and may be published on a NESAS website and it will be provided with an accreditation certificate that formally recognises and records the laboratory’s competency to carry out product security evaluations.

Only after NESAS accreditation has been formally confirmed by GSMA can a security test laboratory conduct network product evaluations under the auspices of the NESAS scheme. NESAS Accreditation of security test laboratories is valid for a period of ISO 17025 accreditation and it is the responsibility of the test laboratory that it keeps its accreditation up to date and renewed by following this process. Failure to do so will cause its NESAS accreditation, and therefore recognition of its competency to conduct network product evaluations, to lapse and become invalid.

Annex A Document Management

A.1 Document History

Version	Date	Brief Description of Change	Editor / Company
0.6	14 Mar 2016	Stable draft presented at SECAG~13 for final review	Bengt Sahlin, Ericsson
0.7	19 Mar 2016	Final draft produced following SECAG#13 to reflect updated definitions and other minor edits	James Moran, GSMA

A.2 Other Information

Type	Description
Document Owner	NESAS Accreditation Board, GSMA SECAG
Editor / Company	Bengt Sahlin, Ericsson

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 security@gsma.com. Your comments or suggestions & questions are always welcome.