Network Equipment Security Assurance Scheme (NESAS) Security Test Laboratory Competency Guidelines

Prepared by GSMA’s Security Assurance Group (SECAG) to help ILAC member accreditation bodies assess the competency of ISO 17025 accredited test laboratories to undertake NESAS product evaluations

April 2020

GSMA HEAD OFFICE
Floor 2
The Walbrook Building
25 Walbrook
London EC4N 8AF
United Kingdom
Tel: +44 (0)20 7356 0600
Fax: +44 (0)20 7356 0601

Table of Contents

1. Introduction..3

1.1 Purpose..3

1.2 Glossary...3

2. Overview...4

3. Evaluator/Evaluation Team Competency 4

4. Testing Equipment and Tools...6

References 7

Abbreviations...7

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 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.

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 17025 accreditation bodies for NESAS Security Test laboratories.

1.2 Glossary

Term	Description
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 17025 Accreditation Body	An ILAC member that is recognised as having competence to carry out ISO 17025 test laboratory audits.
NESAS Security Test Laboratory	A test laboratory that is ISO 17025 accredited in the context of NESAS and that conducts network product evaluations.

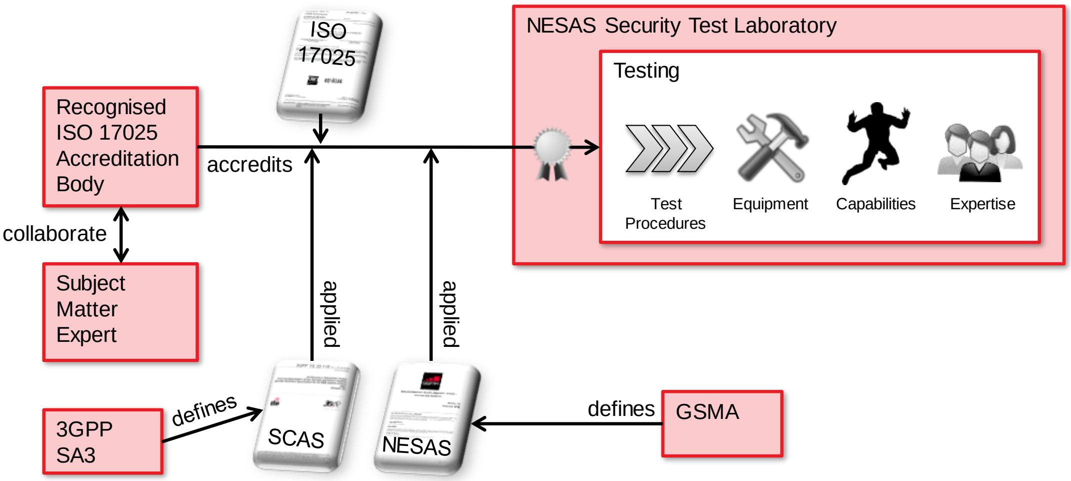
2. Overview

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 process includes the need for the Test Laboratory to demonstrate that it, and specifically the Evaluators assigned by the laboratory, have the ability to execute the test cases defined in the 3GPP Security Assurance Specifications (SCAS) [2] and also 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.

3. Evaluator/Evaluation Team Competency

The requirements and guidance provided below act as supplementary competency requirements to the requirements contained in ISO 17025 and within the NESAS scheme. They are intended to be helpful to experts collaborating and supporting the ISO 17025 accreditation body (so-called Subject Matter Expert). 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 shall be able to demonstrate relevant knowledge of the tasks they are assigned. The Evaluation Team working within the definition of GSMA NESAS is required to:

- Understand the principles and methods used in the GSMA NESAS,
- Understand the relationship between the 3GPP Security Assurance Specification documents and other GSMA NESAS documents used by the scheme,
- Demonstrate an understanding of the overall evaluation planning process (i.e. how to interpret the NESAS 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 the GSMA NESAS (namely to create NESAS Evaluation reports to the level of detail specified in the ISO 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 GSMA 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 an evaluation 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).

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

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

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