MINISTRY OF INTERNATIONAL TRADE AND INDUSTRY
JABATAN STANDARD MALAYSIA

STR 1.15 - SPECIFIC TECHNICAL REQUIREMENTS FOR ACCREDITATION OF NETWORK TESTING LABORATORIES

Issue 1, 13 October 2022

(Supplementary to MS ISO/IEC 17025)

SKIM AKREDITASI MAKMAL MALAYSIA (SAMM)
LABORATORY ACCREDITATION SCHEME OF MALAYSIA

TABLE OF CONTENTS

Introduction

This document describes requirements designed to apply to all types of testing objectives (e.g. safety, performance) and therefore needs to be interpreted with respect to the type of testing concerned and the techniques involved.

This document does not re-state all the provisions of MS ISO/IEC 17025 and laboratories are reminded of the need to comply with all the relevant requirements detailed in MS ISO/IEC 17025. Laboratory is also reminded of the need to comply with any relevant statutory or legislative requirements.

The clause numbers in this document follow those of MS ISO/ IEC 17025 but since not all clauses require interpretation, the numbering may not be continuous.

This document shall be used by Department of Standards Malaysia (Standards Malaysia) to provide appropriate criteria for the assessment and accreditation of laboratories providing evaluation services.

1 Scope

This document shall be read in conjunction with MS ISO/IEC 17025, Accreditation Policy (AP) document, SAMM Policy documents (SP series) and relevant requirements published by Standards Malaysia.

The scope of this document is confined to requirements of conducting network equipment security testing and evaluation for the purpose of accreditation of network testing laboratories.

The scope of accreditation for network testing laboratories performing Network Product evaluation shall confine but not limited to the mobile network technology product applicable for 5G or next generation mobile network technology.

2 Normative references

This document refers to the following standards and the latest editions of the referenced documents (including any amendments) apply: -

i) MS ISO/IEC 17025 - General Requirements for the Competence of Testing and Calibration Laboratories

ii) Accreditation Policy Document

iii) SAMM Policy Documents

iv) MS ISO/IEC 15408-2 - Information technology -- Security techniques -- Evaluation criteria for IT security Part 2 - Security functional Components

v) Network Equipment Security Assurance Scheme (NESAS) Security Assurance Specifications (SCAS).

   a. GSMA FS.13 Network Equipment Security Assurance Scheme – Overview

b. GSMA FS.14 Network Equipment Security Assurance Scheme – Security Test Laboratory Accreditation and Product Evaluation

c. GSMA FS.15 Network Equipment Security Assurance Scheme – Development and Lifecycle Assessment Methodology

d. GSMA FS.16 Network Equipment Security Assurance Scheme – Development and Lifecycle Security Requirements

e. 3GPP TR 33.916 Assurance Methodology for 3GPP network products

f. 3GPP TS 33.117 Catalogue of General Security Assurance Requirements

g. SCAS specific to 3GPP-defined Network Functions

3 Terms and definitions

For the purposes of this document, the relevant terms and definitions below apply;

3.1 3GPP (3rd Generation Partnership Project)

A number of standards organizations which develop protocols for mobile telecommunications.

3.2 Audit Report

Document presenting the results of the Audit conducted at the Equipment Vendor by the Audit Team.

3.3 Configuration Management

A discipline applying technical and administrative direction and surveillance to identify and document the functional and physical characteristics of a configuration item, control changes to those characteristics, record and report change processing and implementation status, and verify compliance with specified requirements.

3.4 Equipment Vendor

Organisation that develops, maintains and supplies to network operators network equipment that supports functions defined by 3GPP.

3.5 Evaluator

Evaluates the network equipment and produces an evaluation report.

3.6 Full evaluation

An evaluation conducted for conformance to the NESAS security requirements for network equipment using test cases.

3.7 GSMA (GSM Association)

An industry organisation that represents the interests of mobile network operators worldwide.

3.8 NESAS (Network Equipment Security Assurance Scheme)

A security assurance framework for the mobile industry, jointly defined by GSMA and 3GPP, that gives a security baseline to evidence that network equipment satisfies a list of security requirements and has been developed in accordance with vendor development and product lifecycle processes that provide security assurance.

3.9 Network Product

Network equipment produced and sold to network operators by an Equipment Vendor.

3.10 Network Product Evaluation

An assessment carried out by a security test laboratory, of network products against the relevant 3GPP defined Security Assurance Specification.

3.11 Software

All or part of the programs, procedures, rules and associated documentation of an information processing system.

3.12 SCAS (Security Assurance Specification)

Specification written by the 3GPP, containing security requirements and test cases for a dedicated 3GPP-defined Network Function or a group of Network Functions.

3.13 Testing

The process of operating a system or component under specified conditions, observing or recording the results, and the process of analysing a network product to detect the differences between existing and required conditions (that is, bugs), and to evaluate the features of the network products.

3.14 Test case

A set of inputs, execution conditions, and expected results developed for a particular objective, such as exercise a particular program path or to verify compliance with a specific requirement.

3.15 Test suite

A set of test scripts or test procedures to be executed in a specific test run.

3.16 Test specification

A document that specifies the test inputs, execution conditions and predicts results for an item to be tested.

3.17 Test tool

Software or hardware that supports one or more test activities.

4 General requirements

Same as in MS ISO/IEC 17025.

5 Structural requirements

Same as in MS ISO/IEC 17025.

6 Resource requirements

6.1 General

6.1.1 The security testing laboratory shall have available the personnel, facilities, equipment, systems and support services necessary to manage and perform its laboratory activities.

Note: Where the laboratory is part of an organisation, support services refer to services obtained from providers outside the organisation as well as services obtained from other division / department within the organisation.

6.2 Personnel

6.2.1 The security testing laboratory shall have sufficient personnel having appropriate technical competency to carry out the testing as prescribed in **Appendix 1** (Personnel Competency Table).

6.2.2 Approved signatory shall comply to the requirements; in Personnel Competency Table and requirements in Standard Malaysia SAMM Policy 6 (SP6) – Requirements for SAMM Approved Signatory. At least 1 year working experience as evaluator in the laboratory or involvement in at least 2 evaluation similar projects of cumulative period of 12 months.

6.3 Facilities and environmental conditions

6.3.1 The word “environment” refers to hardware and associated software, including the required network connection on which the Network Product being tested is running. The security testing laboratory shall ensure that any interference from other activities in the system does not invalidate the result of the specified test.

6.3.2 The laboratory shall have documented procedure to control handling of evaluation performed in an environment controlled by customer, developer or user.

6.3.3 The test environment and the Network Product being tested shall be appropriately monitored, controlled and recorded to ensure valid environmental conditions and correct product identification at all time

6.3.4 Access to facilities, network, operating systems, application and information related to the security testing laboratory activities that may affect the outcome of the testing shall be appropriately controlled from unauthorised personnel. There shall be effective separation of the testing environment including test tools, network connection and Network Product to ensure non-interference for each project.

6.4 Equipment

Same as in MS ISO/IEC 17025.

6.5 Metrological traceability

6.5.1 Same as in MS ISO/IEC 17025.

6.5.2 Same as in MS ISO/IEC 17025.

6.5.3 For Network Product evaluation, “traceability” refers to security evaluation activities which are traceable to the underlying test specification (TS) requirements. This evaluation methodology demonstrates that the tests conducted and the tests assertion made are traceable to TS requirements to ensure that test results constitute credible evidence of compliance.

Where applicable the software test tools shall be calibrated with traceability to national or international standard. For software test tools where calibration is not applicable, the test tools shall be verified before use.

Any measuring instrument used to support the software test tools where the measurement parameters of which have an effect on the validity of the result of the testing shall be calibrated with traceability to national or international standard.

6.6 Externally provided products and services

6.6.1 The security testing laboratory shall use services of an accredited laboratory by Standards Malaysia or laboratory accredited by a signatory to a Mutual Recognition Arrangement such as Asia Pacific Accreditation Cooperation (APAC) and International Laboratory Accreditation Cooperation (ILAC) or licensed by GSMA. Where the externally services provider is not accredited, the laboratory shall evaluate and provide evidence of compliance with the relevant requirements of MS ISO/IEC 17025.

Services can include:

a) testing
b) calibration
c) proficiency testing
d) auditing

6.6.2 The security testing laboratory shall ensure that the evaluator of the external services provider possesses suitable technical competence not less than those stated in **Appendix 1.**

7 Process requirements

7.1 Review of requests, tenders and contracts

7.1.1 For full evaluation, the item(s) to be tested shall have completed the NESAS Scheme audit by GSMA recognised auditor(s) and be accompanied by the audit report.

7.2 Selection, verification and validation of methods

7.2.1 Selection and verification of methods

For full evaluation, the security test laboratory shall conduct the Network Product evaluation using TS requirement in SCAS and where relevant, other supplementary requirements from recognised organisations such as GSMA, 3GPP.

7.2.2 Validation of methods

The security test laboratories shall comply with standards and policies or guidance documents outlined by GSMA and 3GPP.

7.3 Sampling

7.3.1 Within the context of Network Product evaluation, sampling shall refer to the test case selection based on the relevant TS defined by 3GPP unless the laboratory has valid reason for not doing so. Sampling shall include:

a) Selection of test cases to different conditions and combination variables; and
b) Selection of regression tests to run.

7.3.2 Sampling records for testing conducted shall be maintained which includes:

a) Test plan;
b) Test cases and test data selection; and
c) Justification of the selection as in test plan.

7.4 Handling of test items

7.4.1 The interactions between the test items, the test tools and the test environment may result in modification to the Network Product being tested as part of the normal installation or testing process. The security test laboratory shall protect products under evaluation and verified tools used for the evaluation from any modification, unintended use or unauthorised access.

7.4.2 For evaluated product which include software component, the security test laboratory shall ensure that the configuration management mechanisms are in place to prevent unintended modifications to the software components during the evaluation process. Procedure to ensure proper retention, disposal or return of software and hardware after the completion of the evaluation shall be established and maintained.

7.5 Technical records

7.5.1 Screenshot containing the operational results by the tester after the testing shall be taken and maintained by the laboratory.

7.6 Evaluation of measurement uncertainty

7.6.1 For testing in qualitative nature, evaluation of measurement uncertainty is not applicable. The security test laboratory is normally involved in a process of analysis and evaluation rather than measurement, performance of a product or system is not of direct concern to the process of security evaluation. In this context, the concept of 'uncertainty' associated with the commonly understood process of measurement does not apply to ICT security evaluation.

However, in cases where measurement is made during testing such as time delay and expiration time, measurement uncertainty shall be evaluated.

7.7 Ensuring the validity of results

Same as in MS ISO/IEC 17025 and SAMM Policy 4 (SP4) - Policy for Participation in Proficiency Testing Activities.

7.8 Reporting of results

Same as in MS ISO/IEC 17025.

7.9 Complaints

Same as in MS ISO/IEC 17025.

7.10 Nonconforming work

Same as in MS ISO/IEC 17025.

7.11 Control of data and information management

Same as in MS ISO/IEC 17025.

8 Management system requirements

8.1 Options

Same as in MS ISO/IEC 17025.

8.2 Management system documentation

Same as in MS ISO/IEC 17025.

8.3 Control of management system documents

8.3.1 Documents shall include test plans, test suites and test cases. These includes relevant inputs, testing procedures and test design specification which shall be controlled, reviewed and approved. Documents may be suitably classified based on laboratory's identified classification levels (e.g. Top Secret, Secret, Confidential, Restricted and Public) and shall be managed, transferred, stored and disposed in accordance with the procedure appropriate to their classification.

8.4 Control of records

8.4.1 Records may be suitably classified based on laboratory's identified classification levels (e.g. Top Secret, Secret, Confidential, Restricted or Public) and shall be managed, transferred, stored and disposed in accordance with the procedure appropriate to their classification. Laboratories shall have appropriate controls and procedures in place for the collection, storage, manipulation, reduction and transmission of electronic data and results based on their classification level.

8.5 Actions to address risks and opportunities

Same as in MS ISO/IEC 17025.

8.6 Improvement

Same as in MS ISO/IEC 17025.

8.7 Corrective actions

Same as in MS ISO/IEC 17025.

8.8 Internal audits

Same as in MS ISO/IEC 17025.

8.9 Management reviews

Same as in MS ISO/IEC 17025.

Appendix 1

PERSONNEL COMPETENCY TABLE

Role	Academic	Work Experience	Knowledge / Training / Certification	Demonstrable Skills
Evaluator	Any tertiary education (degree/diploma) in any field of telecommunication, network, Information, Communication and Technology (ICT) or equivalent (technical field)	At least 1 year working experience (degree) or at least 3 years working experience (diploma), and a) with a minimum of 6 months experience in ICT security testing (security functional testing, penetration testing, ethical hacking, or related fields) or Experience in performing 1 ICT security testing (security functional testing, penetration testing, ethical hacking, or related fields), b) Successfully completed on the job training programme	Knowledge of MS ISO/IEC 17025 Basic awareness of other standards or bodies of knowledge related to ICT security testing or tools External security testing qualifications (such as Certified Ethical Hacker, SANS Ethical hacker certification, GIAC certifications) or any recognised certification from personnel certification body (such as MBOT and CREST)	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 Be able to analyse the results of the SCAS testing Be able to evaluate evidence (provided by the vendor for the product under evaluation) that the product was developed according to the audited process.

Bibliography

a) MS ISO/IEC 17025:2017 General Requirements for the Competence of Testing and Calibration Laboratories

b) Representing Uncertainty in Physical Security Risk Assessment Considering Uncertainty in Security System Design by Quantitative Analysis and the Security Margin Concept

Acknowledgements

1.	Mr. Pua Hiang (Chairman)	Department of Standards Malaysia
2.	Ms. Norsheda Mohd Bahari (Secretariat)	Department of Standards Malaysia
3.	Mr. Ahmad Dahari Jarno	Cybersecurity Malaysia
4.	Ms. Siti Fatimah Abidin	Cybersecurity Malaysia
5.	Mr. Zef Zalmi Mohamed	Celcom Axiata
6.	Mr. Faisal Md Radi	Celcom Axiata
7.	Mr. Dikhwan Hady Darnalis	Huawei Technologies (Malaysia) Sdn Bhd
8.	Mr. Shamir Amanullah	Lembah Sari Sdn Bhd
9.	Mr. Ashok Sivaji	MIMOS Berhad
10.	Ms. Norahana Salimin	Bank Muamalat Malaysia Berhad
11.	Dr. Kwek Kuan Hiang	Department of Standards Malaysia
12.	Ms. Rosnieh Eggat	Department of Standards Malaysia