Singapore Accreditation Council

ACCREDITATION SCHEME FOR LABORATORIES

IT 001

General Requirements for the Accreditation of Information Technology Security Testing Laboratories

IT 001, 02 April 2018
The SAC Accreditation Programme is managed by Enterprise Singapore

1. Introduction

1.1 This document describes the specific requirements to be complied by Information Technology (IT) Security testing laboratory before they can be accredited.

1.2 This document shall be studied in conjunction with the Document, ISO/IEC 17025 *General Requirements for the Competence of Testing and Calibration Laboratories* and other applicable SAC documents.

1.3 The IT Security Testing includes evaluation of IT Security products [hereafter referred to as Target of Evaluation (TOE)].

See Annex 1 for list of IT security products categories

1.4 Accreditation by SAC or other APLAC/ILAC mutual recognition arrangement (MRA) partners is one of the pre-requisites to be recognized under the Singapore Common Criteria Evaluation and Certification Scheme (*SCCS), administered by Cyber Security Agency (CSA). Accredited laboratory complying with SCCS is deemed able to evaluate Security Targets, and TOE using the Common Evaluation Methodology.

The TOE may be a single product or multiple products configured as an IT product or system solution. By default, the TOE shall be conformant to one or more collaborative Protection Profiles (cPP) approved by the Common Criteria Development Board (CCDB), Protection Profiles approved/published by the Cyber Security Agency of Singapore (CSA). Should there be the case of non-conformance to cPP or National PP, the evaluation shall be performed at most to Evaluation Assurance Level (EAL) 2.

“” Reference documents: SCCS publications available at www.csa.gov.sg.*

2. Terms and Definitions

2.1 The following terms and definitions apply for the purpose of this technical note and the Common Criteria.

(a) Evaluation

The assessment of a Security Target or IT product against a set of Common Criteria requirements using the Common Evaluation Methodology. This term is consistent with the notion of “testing”.

(b) Evaluation Assurance Level (EAL)

A package of Common Criteria assurance requirements that represents a point on the Common Criteria predefined assurance scale. At present, the Common Criteria defines seven hierarchical EALs, from EAL1 to EAL7. IT products which claims conformance to cPP do not have any EAL (i.e. cPP compliant).

(c) IT Security Product

A package of IT software, firmware, and/or hardware, providing security functionality/ies designed for use or incorporation within a multiplicity of systems. An IT product can be a single or multiple IT products configured as an IT system or system solution to meet certain consumer security needs**.**

(d) IT System Solution

Refers to turnkey solution which comprises software applications, infrastructures, hardware and professional services.

(e) Protection Profile (PP)

An implementation-independent set of security requirements for a category of IT products that meet specific consumer needs.

(f) Security Target (ST)

A set of security requirements and specifications to be used as the basis for evaluation under the Common Criteria of an identified Target of Evaluation (TOE). The Security Target specifies an implementation-dependent set of security requirements of the TOE. It also specifies the security objectives, operational environment, threats and any specific security mechanisms that are employed.

(g) Target of Evaluation (TOE)

An IT product or the security relevant part of it and includes its associated administrator and user guidance documentation that is the subject of a security evaluation under the Common Criteria.

3. Laboratory Staff

3.1 Laboratory staff members who conduct IT security evaluation activities shall have the necessary qualifications such as a Bachelor of Science in Computer Science/Information System, Computer Engineering, or related technical discipline or equivalent experience.

3.2 In addition, they shall have relevant knowledge or experience in the following areas: operating systems, data structures, design/analysis of algorithms, database systems, programming languages, computer systems architectures, networking, cryptography, reverse engineering, debugging and experience in and know-how on HW/SW/Cryptographic testing, such as side channel analysis and fault injection.

3.3 Laboratory staff members, who either conducts the IT security evaluation or part of the review and approval chains shall not subject to undue influences or conflict of interests. These includes but not limited to the following:

a. Providing both consultancy and evaluation services for the same TOE;

b. Be concurrently employed/appointed in another unit of the organization or another organization which develops IT Product(s).

c. Own shares of organization which develops IT Product(s).

d. Develop IT Product(s) for public circulation or commercial purposes.

3.4 Nominees for approved signatories shall meet the requirements stipulated in Clause 5 of SAC-SINGLAS 001 Accreditation Process.

3.5 Nominees of approved signatories shall pass the CSA’s written assessment for IT Security Personnel before SAC’s assessment is conducted.

4. Equipment

4.1 Computer systems and other platforms used during the conduct of testing shall be under configuration control. The laboratory shall have procedures to ensure that any equipment (hardware and software) used for testing is in known state prior to use for testing.

5. Measurement Traceability

5.1 For Common Criteria testing, “traceability” is interpreted to mean that security evaluation activities are traceable to the underlying Common Criteria requirements and work units in the Common Evaluation Methodology. This means that test tools and evaluation methodology demonstrate that the test they conduct and the test assertions they make are traceable to specific criteria and methodology.

6. Handling of test items

6.1 The laboratory shall have physical, logical and procedural controls to ensure that access to test items are granted only to the laboratory staffs and on a need-to-know basis.

7. Demonstration of Competence

7.1 Laboratory shall have adequate set-up (i.e. hardware/software) to conduct the test during SAC assessment. A demonstration of evaluation of all the applied product categories shall be conducted.

Annex 1

IT Security Products Categories

a) Access Control Devices and Systems

b) Biometric Systems and Devices

c) Boundary Protection Devices and Systems

d) Data Protection

e) Databases

f) Detection Devices and Systems

g) ICs, Smart Cards and Smart Card-Related Devices and Systems
  - IC
  - Platform
  - ICC

h) Key Management Systems

i) Mobility

j) Multi-Function Devices

k) Network and Network-Related Devices and Systems

l) Operating Systems

m) Other Devices and Systems

n) Products for Digital Signatures

o) Trusted Computing