# ISCB PRODUCT CERTIFICATION SCHEMES POLICY (PRODUCT_SP)

File name: ISCB-5-POL-11-PRODUCT_SP-v1a
Version: v1a
Date of document: 19 JUNE 2017
Document classification: PUBLIC

For general inquiry about us or our services,
please email: info@cybersecurity.my



CyberSecurity Malaysia
(726630-U)
Corporate Office:
Level 5, Sapura@Mines
No 7, Jalan Tasik
The Mines Resort City
43300 Seri Kembangan
Selangor Darul Ehsan
Malaysia.
T +603 8992 6888
F +603 8992 6841
H 1 300 88 2999
www.cybersecurity.my

# ISCB PRODUCT CERTIFICATION SCHEMES POLICY (PRODUCT_SP)

19 JUNE 2017

ISCB Department

**CyberSecurity Malaysia**

Level 5, Sapura@Mines | No 7 Jalan Tasik,

The Mines Resort City | 43300 Seri Kembangan, Selangor

Tel: +60 (0)3 8992 6888 | Fax: +60 (0)3 8945 3205

http://www.cybersecurity.my

# Document Authorisation

| | |
|---|---|
| ***DOCUMENT TITLE:*** | ISCB PRODUCT CERTIFICATION SCHEMES POLICY (PRODUCT_SP) |
| ***DOCUMENT REFERENCE:*** | ISCB-5-POL-11-PRODUCT_SP-v1a |
| ***ISSUE:*** | v1a |
| ***DATE:*** | 19 JUNE 2017 |

***PREPARED BY:***

| | |
|---|---|
| Amiroul Farhan Roslaini<br>Executive, ISCB Department<br>CyberSecurity Malaysia | Date |

***REVIEWED BY:***

| | |
|---|---|
| Wan Shafiuddin Zainuddin<br>Head, ISCB Department<br>CyberSecurity Malaysia | Date |

***APPROVED BY:***

| | |
|---|---|
| Dato' Dr Hj Amirudin Abdul Wahab<br>Chief Executive Officer<br>CyberSecurity Malaysia | Date |

***DISTRIBUTION:*** UNCONTROLLED COPY

# Forward

The Information Security Certification Body (ISCB), a department within CyberSecurity Malaysia, has a mission to become a national certification body that provides comprehensive cyber security evaluation and certification services which include product/technology, process, and professional certifications. These certification services will measure the effectiveness of the cyber security implementation in an organisation and will contribute to the effectiveness and efficiency of operations, reliability and durability, and information security compliance.

This document provides an overview of the product certification schemes operated by ISCB and specifies the business rules governing its operation.

Dr. Amirudin Abdul Wahab

Chief Executive Officer

CyberSecurity Malaysia

All correspondence in connection with this document should be addressed to:

Head of ISCB Department

CyberSecurity Malaysia

Level 7, Sapura@Mines

No 7 Jalan Tasik

Mines Resort City,

43300 Seri Kembangan,

Selangor

# Copyright Statement



Registered office:

Level 5, Sapura@Mines,

No 7 Jalan Tasik, The Mines Resort City,

43300 Seri Kembangan

Selangor Malaysia

Registered in Malaysia – Company Limited by Guarantee

Company No. 726630-U

*Printed in Malaysia*

# Trademarks

All terms mentioned in this document that are known to be trademarks or service marks have been appropriately capitalised. CyberSecurity Malaysia cannot attest to the accuracy of this information. Use of a term in this document should not be regarded as affecting the validity of any trademark or service mark.

# Disclaimer

Every effort has been made to make this document as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an "as is" basis. The author and CyberSecurity Malaysia shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this document.

Certification increases the assurance and reduce the risk of exploitable vulnerabilities. There will remain a small level of risk that exploitable vulnerabilities remain undiscovered which come from outside of the certification scope. Information about the certified product, organisation, or people is made available by CyberSecurity Malaysia for the purpose of advising and assisting interested parties on matters relating to the security and integrity of information that is processed, stored or communicated by electronic or similar means using communications and computer technologies. The information that CyberSecurity Malaysia provides in relation to the certified product, organisation, or people is limited to the scope of the certification against the recognised certification criteria.

# Document Change Log

| RELEASE | DATE | PAGES AFFECTED | REMARKS/CHANGE REFERENCE |
|---|---|---|---|
| v1 | 1 MARCH 2017 | All | Final released. |
| v1a | 19 JUNE 2017 | 7, 9, 10, 11, 13, 14, 15, 21, 23, 25 | Incorporate information regarding MTSEAL (additional comments received on 12 April 2017). |

# Table of Contents

.

# Index of Tables



# Index of Figures

# 1 Introduction

## 1.1 Purpose

1 This policy document (PRODUCT_SP) provides an overview of the product certification schemes operated by the Information Security Certification Body (ISCB) and specifies the business rules governing its operation.

2 The intended audience for this document is any party interested in gaining a general understanding on the product certification schemes operated by ISCB. More detailed information on the operation of the product certification schemes, and the conduct of certification and evaluation activities, can be found in specific certification schemes publications. These other official ISCB product certification schemes publications are:

a) The ISCB Evaluation Facility Manual (ISCB_EFM) that provides interpretation of this policy applicable for the management and operation of licensed Security Evaluation Facilities (SEFs); and

b) The ISCB Certification Scheme Register (refer to Section 2.4) that lists all ISCB certifications and evaluation projects.

3 Other official publications that provide detailed guidance for the aspects of ISCB product certification schemes operation that are not publicly available are:

a) The ISCB Product Certification Manual (PRODUCT_CM) that provides interpretation of this policy application for the management and operation of ISCB Product Certification Scheme Section as specifies in Section 2.4 of this document;

b) ISCB product certification processes specific to the certification schemes operated by the units (or known as the certification bodies) under the ISCB Product Certification Scheme Section (refer Section to 2.4) that cover the details of Accept, Execute, and Certify phases; and

c) The ISCB Product Certification Quality & Security Manual (PRODUCT_QSM) and ISCB Product Certification Procedures Manual (PRODUCT_PM) that defines the quality and information security management system (QISMS) for operation of the ISCB Product Certification Scheme Section.

4 Third parties seeking access to documents that are not publicly available must submit a request in writing to the Head of ISCB Department. The decision to release these documents to a third party is at the discretion of ISCB and may be subject to conditions as part of that release.

## 1.2 Document

5 This policy will, where applicable, make references to other ISCB product certification schemes publications. ISCB personnel may access the current version of these referenced documents or records from the public area of ISCB.

### 1.2.1 Scope

6 This policy applies to the operation of the ISCB Product Certification Scheme Section which includes the certification bodies of the product certification schemes, any Security Evaluation Facility licensed to conduct evaluations under the ISCB product certification schemes, and ISCB customers.

### 1.2.2 Document Organisation

7 This policy document is organised into the following sections:

a) **Section One** provides an introduction to the policy, and describes the purpose and scope of the document.

b) **Section Two** provides an overview and background of the ISCB product certification schemes services.

c) **Section Three** provides the ISCB product certification schemes structure, and outlining high level roles and responsibilities.

d) **Section Four** provides rules and requirements on the conduct of the ISCB product certification schemes services.

e) **Annex A** lists the references and terminology relevant to this document.

f) **Annex B** states the rules for ISCB product certification and service marks.

### 1.2.3 Changes to this Policy

8 The change authority for this document is the Scheme Head. All change requests in relation to the policy should be forwarded in writing to the Head of ISCB Department.

9 All changes will be submitted to the Scheme Head for final approval.

10 Changes to this document should be managed in accordance with the ISCB Product Certification Quality & Security Manual (PRODUCT_QSM) (Ref [11]) and ISCB Product Certification Procedures Manual (PRODUCT_PM) (Ref [12]).

11 All approved changes to this policy will be published on the respective certification schemes website as stated in Section 2.4 of this document.

### 1.2.4 Document Relationships

12 The relationship between this policy (shown in red) and other documents in the hierarchy is illustrated in Figure 1 below.

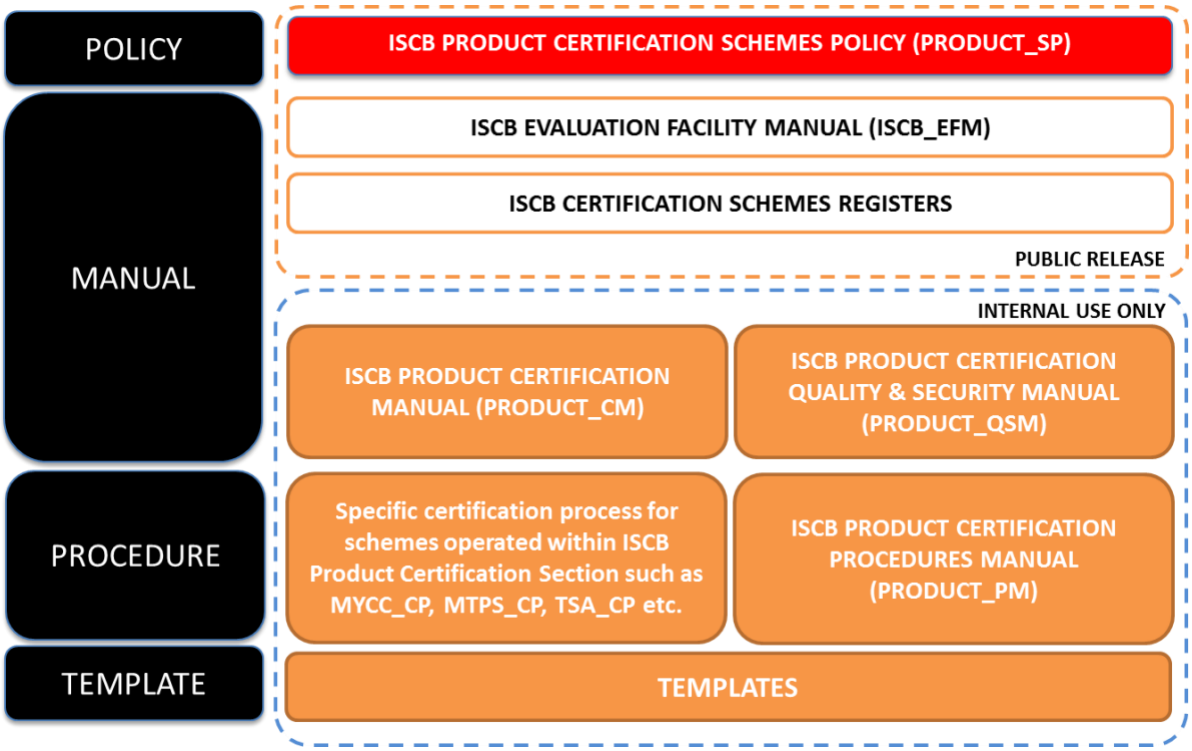


Figure 1: Document Relationships for ISCB Product Certification Scheme Section

# 2 ISCB Product Certification Schemes Overview

## 2.1 Background

13 Most organisations rely on technology to store, process and transfer information. Therefore, organisations need to identify, prioritise and manage security risks to their information. They need to identify context, determine the threats, consider their impact to the organisation if the threat is realised, and determine those risks that require control. However, most organisations have limited resources to concentrate on information security problem. Business structure and operating models differ from one organisation to another.

14 Controls may be implemented in technology, facilities and infrastructure, policies and procedures, and people. But how can the organisation know that the security controls are effective? The organisation needs a culture of security at levels appropriate to the business, and continuously test the security implementation. This provides the basis for assurance, and it provides confidence in implementing security controls.

15 Assurance is the basis for confidence or trust in something. In information security, assurance means confidence that the organisation is protected against security threats, confidence in the implementation of security controls, and confidence in the security functions implemented by a product or system.

16 An independent security evaluation and certification conducted by a trusted party, that covers product/technology, process, and people, is a method of gaining confidence in the security implementation.

17 In response to these business drivers, Information Security Certification Body (ISCB), a department within CyberSecurity Malaysia, has a mission to become a national certification body that provides comprehensive cyber security evaluation and certification services which include product/technology, process, and professional certifications. These certification services will measure the effectiveness of the cyber security implementation in an organisation and will contribute to the effectiveness and efficiency of operations, reliability and durability, and information security compliance.

## 2.2 Applicable Legislation Policy and Standards

### 2.2.1 National Cyber Security Policy

18 CyberSecurity Malaysia implemented the National Cyber Security Policy (NCSP) to accumulate the national effort for enhancing the security of Malaysia's Critical National Information Infrastructure (CNII). The guiding vision for the NCSP is:

> **Malaysia's Critical National Information Infrastructure shall be secure, resilient and self-reliant. Infused with a culture of security it will promote stability, social well-being and wealth creation.**

19 The NCSP identifies eight policy thrusts:

a) Effective Governance;

b) Legislative and Regulatory Framework;

c) Cyber Security Technology Framework;

d) Culture of Security and Capacity Building;

e) Research and Development Towards Self-Reliance;

f) Compliance Enforcement;

g) Cyber Security Emergency Readiness; and

h) International Co-operation.

20 The ISCB product certification schemes provide key programs within the Cyber Security Technology Framework of the NCSP that will fulfil the implementation of:

a) an evaluation and certification programme for ICT security products and systems, and

b) Information Security standards among CNII agencies or organisations, and to ensure compliance through the certification schemes services.

### 2.2.2 Malaysian Government Cabinet Decision

21 The establishment of product certification schemes operated by ISCB was inspired by the Malaysian Government Cabinet decisions as follows:

a) **Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme**

On 8 October 2008, Malaysian Government Cabinet considered the Memorandum No. 592/2618/2008 from Ministry of Science, Technology and Innovation (MOSTI) and agreed:

i) To appoint CyberSecurity Malaysia, an agency under Ministry of Science, Technology and Innovation (MOSTI), as the sole Certification Body for the Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme, and IT security evaluation under the CCRA.

ii) The Certification Body will be named as Malaysian Common Criteria Certification Body (MyCB).

b) **Malaysia Trustmark**

CyberSecurity Malaysia has been entrusted to become the Operator and Certifier for Malaysia Trustmark for Private Sector through the Memorandum Jemaah Menteri No. 945/2717/2010 dated 26 November 2010.

### 2.2.3 International Obligations

22 The Malaysian Government, through CyberSecurity Malaysia and the MyCC Scheme is a signatory to the Common Criteria Recognition Arrangement (CCRA) (Ref [1]). The CCRA is an agreement between countries that establishes the rules and requirements for security evaluations such that results of these evaluations are recognised across all member countries. Participation in this agreement places specific obligations on the operation of the MyCC Scheme, namely:

a) **Voluntary periodic assessment**: To provide assurance that the MyCC Scheme maintains competency and is compliant with CCRA rules, the scheme is subject to assessment by other CCRA member nations for:

i) MyCC Scheme entry as a certificate authoriser under the CCRA; and then

ii) At least every five years from acceptance as a certificate authoriser under the CCRA.

b) **Management system**: The MyCB and MySEFs must operate a management system. The MyCB operates it management system to ensure that ISO/IEC 17065 and CCRA requirements are met. MySEFs must be accredited as compliant with the requirements of ISO/IEC 17025 for evaluation services as described in paragraph 28a) and 28b)[1].

c) **Scheme Authority**: Each member country may have only one government body as the entity responsible for the scheme. CyberSecurity Malaysia is the only Malaysian government body that has the authority to operate an ICT security evaluation and certification scheme within Malaysia. The Chief Executive Officer of CyberSecurity Malaysia is the head of the MyCC Scheme.

d) **Competency**: The MyCC Scheme must ensure that suitable technical competency in ICT security certification and evaluation is maintained to support operations. CyberSecurity Malaysia as the operator of the MyCC Scheme ensures that suitable technical competency is maintained within the MyCB and by licensed MySEFs. Further, the MyCB provides oversight of MySEF evaluators to ensure that evaluation criteria and methodology are correctly applied.

## 2.3 CyberSecurity Malaysia's Role

23 CyberSecurity Malaysia has evolved from its beginnings in 1997 as the Malaysian Computer Emergency Response Team (MyCERT) addressing computer security issues amongst Malaysian Internet users. In 1998 the National IT Council (NITC) meeting directed that an agency be formed to address Information and Communication Technology (ICT) security issues in Malaysia establishing the National ICT Security & Emergency Response Centre (NISER) that would encapsulate MyCERT. In 2005, a cabinet decision determined that NISER is being established as a Non-Profit Company Limited by Guarantee reporting to Ministry of Science, Technology and Innovation (MOSTI). On the 20th August 2007, CyberSecurity Malaysia was launched by the Prime Minister and operates as a not for profit government owned company by MOSTI.

24 As a not-for-profit company, CyberSecurity Malaysia derives its funding through allocations from the Malaysian Government for the implementation of components of the Malaysian Plan and the National Cyber Security Policy.

25 The mission of CyberSecurity Malaysia is **to create and sustain a Safer Cyberspace to Promote National Sustainability, Social Well-Being and Wealth Creation**. The certification schemes are impartially operated by CyberSecurity Malaysia as a component of its security assurance services.

[1] Note that this does not preclude an evaluation facility being accredited for additional evaluation or testing services.

26 CyberSecurity Malaysia recovers costs for the delivery of its product certification schemes services through a fee for service charging model. The fee structure for ISCB product certification schemes services are published at the respective product certification schemes website as stated in Section 2.4 of this document.

## 2.4 ISCB Product Certification Schemes Services

27 The product certification schemes operated by ISCB include:

a) Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme (website: http://www.cybersecurity.my/mycc)

b) Malaysia Trustmark for Private Sector (MTPS) (website: http://mytrustmark.cybersecurity.my)

c) Technology Security Assurance (TSA) Scheme (website: *currently under development*)

d) Cryptographic Module Validation Program (MyCMVP) (website: *currently under development*)

e) MyTrustSEAL (MTSEAL) Scheme (website: *currently under development*)

### 2.4.1 Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme

28 MyCC Scheme SHALL offer the following certification and evaluation services to customers:

a) **Security evaluation and certification of ICT products and systems (called a target of evaluation (TOE))** – Impartial assessment of the security of a TOE against a set of functional and assurance claims using CC (Ref [2], [3], [4]) and CEM (Ref [5]) and in conformance with ISCB product certification schemes rules (Section 4). Certification provides independent confirmation of the validity of evaluation results and that the TOE meets its security requirements at a defined level of assurance. No other endorsement is given or implied by this certification. This service provides customers confidence in the security functionality provided by a TOE.

b) **Security evaluation and certification of CC protection profiles (PPs)** – Impartial assessment of an implementation independent set of security requirements to determine whether they solve a stated security problem. This assessment uses CC (Ref [2], [3], [4]) and CEM (Ref [5]) and in conformance with ISCB product certification schemes rules (Section 4). Certification provides independent confirmation of the validity of evaluation results and a level of confidence that the protection profile solves the stated security problem. No other endorsement is given or implied by this certification. This service provides customers with validated security requirements to support selection and procurement of ICT products.

c) **Maintenance of assurance for security certified ICT products and systems** – Services that provide maintenance of a level of assurance in those ICT products that have completed security certification within the MyCC Scheme and in conformance with ISCB product certification schemes rules (Section 4). This

service provides customers with a cost effective method of maintaining a level of confidence in the security provided by a TOE as it is updated.

d) **Recognition of CCRA certificates for special purposes** – Services that facilitate the recognition of an ICT product that has been security certified externally to the MyCC Scheme under the CCRA (Ref [1]) where specific Malaysia national security policy requirements may apply. This service provides customers with specific Malaysian national security requirements confidence that CC certified ICT products from other schemes meet these requirements.

29 MyCC Scheme certification applies only to a specific version of a TOE. Maintenance of assurance is a voluntary process that leverages a certified TOE baseline as changes are made to the certified TOE. Consumers of a certified TOE should make their own risk-based decisions on the use or otherwise of these products or systems.

30 Malaysian Common Criteria Certification Body (MyCB) Unit is the certification body that is responsible to manage the operation of the MyCC Scheme.

31 MyCB shall employ the following internationally standard for conducting MyCC Scheme IT security evaluation:

a) Common Criteria for Information Security Technology Evaluation (CC) (Ref [2], [3], [4]) which consist of three parts:

i) Part 1: Introduction and general model (Ref [2]);

ii) Part 2: Security functional components (Ref [3]; and

iii) Part 3: Security assurance components (Ref [4]).

32 MyCB shall use the Common Evaluation Methodology for Information Technology Security Evaluation (CEM) (Ref [5]) as the accepted IT security evaluation methodology that supports the correct application of CC.

33 As a participant of the CCRA, MyCB will always use the official current version of the CC and CEM available on the CCRA portal (www.commoncriteriaportal.org).

34 The ICT products, systems, and protection profiles that have been certified or that are in evaluation under MyCC Scheme will be published in the MyCC Scheme Certified Products Register (MyCPR) at www.cybersecurity.my/mycc.

### 2.4.2 Malaysia Trustmark for Private Sector (MTPS)

35 MTPS SHALL offer the following certification and evaluation services to customers:

a) **Security audit ad validation of an organisation's e-business** – Impartial audit and validation of an organisation based on legality of the organisation and security controls of the e-business website and transactions. The organisation will be assessed using five (5) domains as the basis of MTPS checklist. The five domains are:

i) Domain 1: disclosure of information

ii) Domain 2: practices

iii) Domain 3: security

iv) Domain 4: customer data protection

v) Domain 5: alternative dispute resolution (ADR)

Audit and validation provides independent confirmation of the audit results and that the organisation is in conformance with the ISCB product certification schemes rules (Section 4). The service provides an organisation with an increase level of trust with respect to it e-business.

36 The validity of Malaysia Trustmark is one (1) year. Organisations need to re-apply if they want to continue using the Malaysia Trustmark.

37 MTPS shall employ the World Trustmark Alliance (WTA) Code of Conduct (Ref [8]), and related Malaysia acts, policies, standards and best practices in developing the MTPS technical requirements.

38 Malaysia Trustmark Operator (MTO) Unit is the certification body that is responsible to manage the operation of MTPS.

39 The organisation e-business website and transactions that have been validated under the MTPS will be published in the MTPS Validated Website Register (MTPS_VWR) at http://mytrustmark.cybersecurity.my.

### 2.4.3 Technology Security Assurance (TSA) Scheme

40 Technology Security Assurance (TSA) Scheme SHALL offer the following certification and evaluation services to customers:

a) **Security evaluation and certification of ICT products (called a target of evaluation (TOE))** – Impartial security assessment that shall include:

i) Functional testing and vulnerability assessment of the TOE against TSA Mandatory Security Functions Requirement (TSA_MSFR) which is developed based on the international standards and best practices such as the CC (Ref [2], [3], [4]) and other related best practices.

ii) Cryptography conformance and randomness testing; only for ICT product that claims cryptography function.

The evaluation above shall conform to ISCB product certification schemes rules (Section 4). Certification provides independent confirmation of the evaluation results' validity and that the TOE meets its security requirements. No other endorsement is given or implied by this certification. This service provides customers confidence in the security functionality provided by a TOE.

b) **Certification maintenance** – services that provide confidence in those ICT products that have completed security certification within TSA Scheme and in conformance with ISCB product certification schemes rules (Section 4). This service is mandatory in order to maintain the certification and to ensure a level of confidence in the security provided by the certified ICT product and its operational environment as it is updated. Security posture assessment (SPA) of the ICT product and its operational environment shall be conducted annually. Through this value added service, the risk of malicious or accidental access to data managed by the certified ICT product shall be reduced. During the SPA, if the assessment team found that the version of the certified product has changed, then the product shall be submitted to ISCB for recertification.

41 TSA Scheme certification applies only to a specific version of a TOE and is valid for one (1) year. Certification maintenance is a compulsory process (shall be conducted annually) in order to maintain or continue the certification.

42 TSA Scheme shall employ the same standards and methodology use by MyCC Scheme. However, ISO/IEC 19790 (Ref [6]) shall be used as an additional standard for conducting IT security evaluation if the strength of the cryptographic module provided by the TOE need to be evaluated.

Note. MyCC Scheme does not evaluate the strength of the cryptographic module.

43 The ISO/IEC 24759 (Ref [7]) shall be used by ISCB as the accepted IT security evaluation methodology that supports the correct application of ISO/IEC 19790 (Ref [6]).

44 TSA Certification Body (TSACB) Unit is the certification body that is responsible to manage the operation of TSA Scheme.

45 The ICT products and its operational environment that have been certified or that are in evaluation under TSA Scheme will be published in the TSA Scheme Certified Products Register (TSA_CPR) at TSA Scheme website which is currently under development.

### 2.4.4 Cryptographic Module Validation Program (MyCMVP)

46 MyCMVP is currently under development as one of ISCB 11th Malaysian Plan project. The details of MyCMVP services will be updated once the scheme is ready for operation.

47 MyCMVP shall employ ISO/IEC 19790 (Ref [6]) for conducting IT security evaluation.

48 The ISO/IEC 24759 (Ref [7]) shall be used by ISCB as the accepted IT security evaluation methodology that supports the correct application of ISO/IEC 19790 (Ref [6]).

49 MyCMVP Certification Body (MyCMVP_CB) Unit is the certification body that is responsible to manage the operation of MyCMVP.

50 The ICT products that have been certified or that are in evaluation under MyCMVP will be published in the MyCMVP Certified Products Register (MyCMVP_CPR) at MyCMVP website which is currently under development.

### 2.4.5 MyTrustSEAL (MTSEAL) Scheme

51 MTSEAL Scheme is currently under development as one of the ISCB service collaborating with CSM strategic partner to recognise a website based on content media assessment and web security validation. The details of MTSEAL Scheme services will be updated once the scheme is ready for operation.

52 MTSEAL Scheme shall adopted WTA Code of Conduct [8] as reference to develop it scheme's principles. MTSEAL Scheme will also employ the Malaysian Communications and Multimedia Content Code, a self-regulation by the industry in compliance with the Communications and Multimedia Act 1998 (CMA 98).

53 MTSEAL Certification Body (MTSEAL_CB) Unit is the certification body that is responsible to manage the operation of MTSEAL Scheme.

54 The website that have been validated under the MTSEAL Scheme will be published in the MTSEAL Scheme Certified Website Register (MTSEAL_CWR) at MTSEAL Scheme website which is currently under development.

### 2.4.6 Limitations on Certification

55 Certification is not a guarantee that a certification scope is completely free of exploitable vulnerabilities. There will remain a residual level of risk that exploitable vulnerabilities remain undiscovered in its claimed certification scope. This residual risk is reduced through the continuous evaluation by the certification scheme to ensure level of assurance in the security provided by the certified ICT product, website, or e-business with respect to its defined certification scope.

56 Certification applies only to a specific certification scope such as version of a TOE, or a website. No claims can be made in relation to other certification scope unless they have been independently evaluated and certified, or have been formally recognised through related ISCB product certification schemes surveillance or certificate maintenance services.

57 Specific surveillance activities will be conducted only for ISCB product certification schemes which provide surveillance or certificate maintenance services. This is to ensure ongoing compliance with the ISCB product certification scheme rules (Section 4). ISCB product certification schemes which have no specific surveillance services, such as MyCC, MTPS and MTSEAL, surveillance activities will not be conducted on the certified products, but for the use of certificate marks or logos.

## 2.5 Supporting Services

58 To support the delivery of ISCB product certification schemes services, ISCB shall deliver the following additional services:

a) Secretariat Services – the process that provides the secretariat services to the ISCB Scheme Management Board (ISMB), and other activities as determined by the Scheme Head;

b) Publications Management – provides configuration and content management of ISCB product certification schemes publications, websites, and certification registers;

c) Security Evaluation Facilities Licensing and Management – manages the relationship between CyberSecurity Malaysia with current and prospective Security Evaluation Facilities;

d) Interpretations Management – manages all current and proposed interpretations of ISCB product certification schemes criteria, rules and publications;

e) CCRA Engagement – manages MyCC Scheme engagement with the CCRA member countries, and participation in the development and maintenance of the CCRA (Ref [1]), CC (Ref [2], [3], [4]) and CEM (Ref [5]) on behalf of the Malaysian Government;

f) Training and Development – defines and manages the delivery of certification and relevant training programs;

g) Operation and maintenance of ISCB product certification schemes quality and security management system; and

h) Provision of support to third party assessors for the purpose of assessing compliance of the ISCB product certification schemes such as:

   i) MyCC Scheme with CCRA requirements (Voluntary periodic assessment) (Ref [1]), and

   ii) accreditation of license Security Evaluation Facilities against ISO/IEC 17025 (Ref [10]).

# 3 ISCB Product Certification Schemes Structure

59 ISCB product certification schemes provide a model for certifying product, technology, website, or e-business against internationally recognised cyber security standards and best practices.

60 An overview of the ISCB product certification schemes structure is illustrated in Figure 2 below.

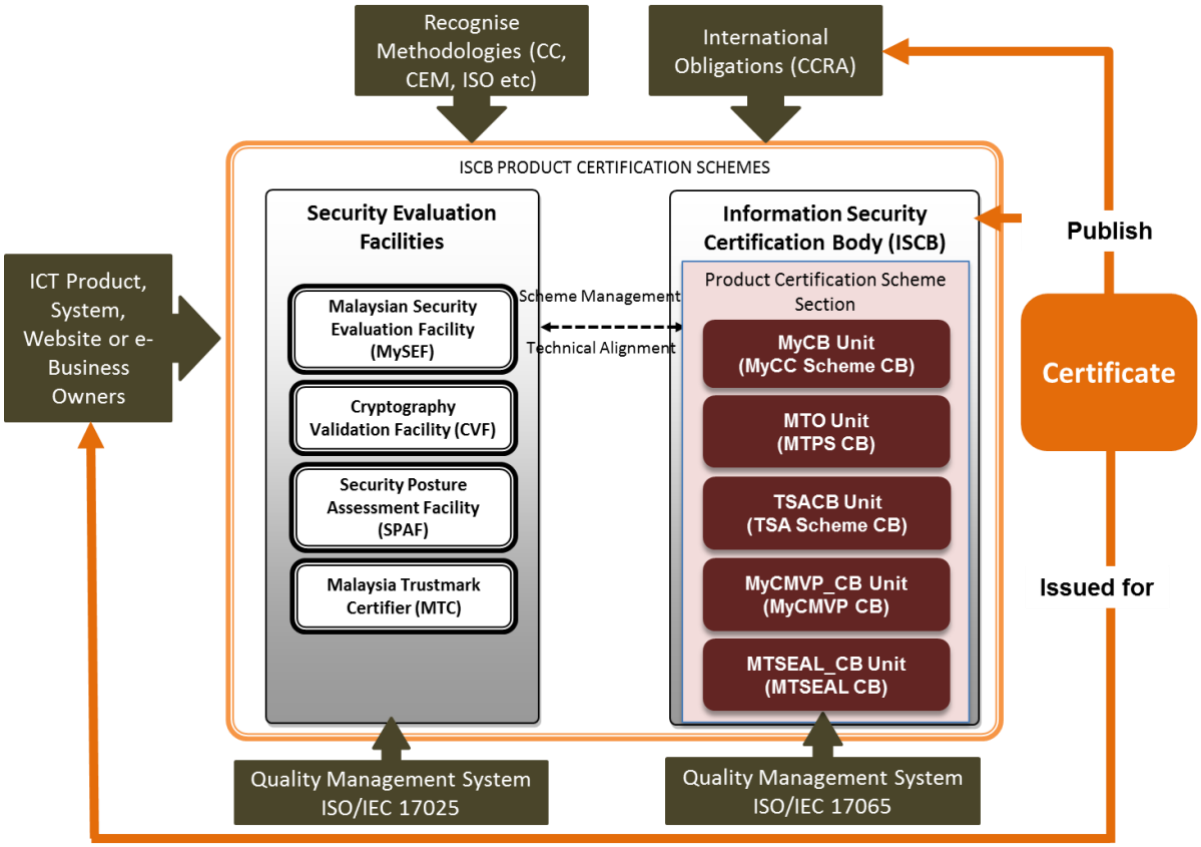


Figure 2: ISCB Product Certification Schemes Structure

61 An overview of ISCB product certification schemes had been discussed in Section 2 of this document. Therefore, this section will outline only the high level roles and responsibilities of the two important roles within ISCB product certification schemes: the certification bodies of the schemes and the licensed Security Evaluation Facility.

## 3.1 Certification Bodies of the ISCB Product Certification Schemes

62 Units within ISCB Product Certification Scheme Section are responsible to manage the operation of the schemes and certifies the evaluation results (refer Figure 2).

63 The certification bodies monitor the evaluation process, interacting with the Security Evaluation Facilities where necessary, and providing independent oversight activities to ensure that the evaluation process is conducted in accordance with the requirements of the product certification schemes rules (Section 4). The certification bodies issue a certificate for those products, systems, protection profiles, websites, or e-businesses that meet the requirements of the IT security evaluation criteria. The overall evaluation and certification process is illustrated in Figure 3.

64 While one person can fill more than one role, the certification body is required to maintain a minimum of two staff to ensure that appropriate reviews are performed.

65 Each certification body of the ISCB product certification schemes shall be composed of the following elements:

a) **Scheme Manager** - This role is responsible for the general management of respective certification schemes services, and the relationship and interface with licensed Security Evaluation Facilities and/or external parties such as external assessors (if any). In addition, the Scheme Manager is responsible:

i) to ensure minimum staffing levels and competency are maintain to sustain the operation of the respective certification body and within licensed Security Evaluation Facilities including career and technical development;

ii) to ensure that new and existing personnel within the respective certification scheme is free from any actual or potential conflict of interest in the performance of their duties; and

iii) to provide respective certification scheme's certification or audit reports to the Scheme Head for certification consideration.

While one person can fill more than one role, each certification body will have only one staff member nominated as the Scheme Manager.

Ideally, the Scheme Manager will also have evaluation skills equivalent to the Senior Certifier role.

b) **Senior Certifier** - This role is responsible for:

i) Ensuring the effective application of IT security evaluation criteria by both evaluators and certifiers;

ii) Ensuring that the highest standards of competence and impartiality are maintained, and that consistency is achieved across all evaluation and certification activities;

iii) The relationship and interface with the Senior Evaluator(s) of the licensed Security Evaluation Facility(s);

iv) Planning the technical development of the certifiers;

v) The continuous application of ISCB product certification schemes quality and security management system, and certification schemes' procedures to the conduct of all certification activities; and

vi) Review and sign certification reports as the senior technical certification expert and providing such reports to the Scheme Manager.

While one person can fill more than one role, each certification body will have only one staff member nominated as the Senior Certifier.

c) **Certifier/ MTPS Operator** – This role is responsible for the conduct of day-to-day product certification schemes services under the direction of the Scheme Manager and/or Senior Certifier and in compliance with the ISCB product certification schemes quality and security management system, and certification schemes' procedures. The Certifier/ Operator signs certification or audit reports for only those certification projects that they perform the certification role.

## 3.2 Licensed Security Evaluation Facilities

66 ISCB shall license suitably qualified commercial or government entities who are independent entity from ISCB to conduct information security testing, inspection, and evaluation in accordance with the requirements of the ISCB product certification schemes rules (Section 4). A listing of licensed Security Evaluation Facilities is published at the respective product certification schemes website as stated in Section 2.4 of this document.

67 Any commercial or government entity may apply to become a Security Evaluation Facility. Only those that:

a) Satisfy the ISCB requirements (requirements are specified in the ISCB Evaluation Facility Manual (ISCB_EFM) (Ref [14]); and

b) Submit an application, in the form of a letter or proposal document, that demonstrates they can meet all the requirements for operating as a Security Evaluation Facility;

can be awarded a license to operate as a Security Evaluation Facility.

68 Security Evaluation Facilities licensed by ISCB to deliver the IT security evaluation are categorised as follows:

a) Malaysian Security Evaluation Facility (MySEF) – evaluation facility that is licensed by ISCB to conduct security evaluations of ICT products, systems, and protection profiles against CC (Ref [2], [3], [4]) and CEM (Ref [5]);

b) Cryptography Validation Facility (CVF) – evaluation facility that is licensed by ISCB to conduct cryptography conformance and randomness testing against ISO/IEC 19790 (Ref [6]) and ISO/IEC 24759 (Ref [7]);

c) Security Posture Assessment Facility (SPAF) – organisation or facility that is licensed by ISCB to deliver security posture assessment (SPA) of the certified ICT product's operational environment; and

d) Malaysia Trustmark Certifier (MTC) – organisation or facility that is licensed by ISCB to conduct Trustmark Technical Security Assessment (TTSA) i.e. to validate the security aspects of the e-business web portal and online payment system against the MTPS technical requirements and additional adopted standards such as PCI-DSS and web security best practices (OWASP).

Note. The security evaluation facilities above may be provided by the same organisation.

69 MySEF(s) and CVF(s) shall obtained ISO/IEC 17025 (Ref [10]) accreditation from Jabatan Standards Malaysia or other accreditation authorities who are recognised by the Malaysian government and CyberSecurity Malaysia for the performance of information security testing, inspection and evaluation against the CC (Ref [2], [3], [4]), CEM (Ref [5]), ISO/IEC 19790 (Ref [6]), and ISO/IEC 24759 (Ref [7]).

70 For SPAF and MTC, it is optional to obtain ISO/IEC 17025 accreditation. However, they shall meet the requirements specified in Annex B of the ISCB Evaluation Facility Manual (ISCB_EFM) (Ref [14]) or the requirements of ISO/IEC 17025. ISCB is responsible to determine the compliance against the requirements during the licensing site visit.

71 Each licensed Security Evaluation Facility maintains, as a minimum, the following roles:

a) **Security Evaluation Facility Manager** – This role is responsible for the general management of the facility personnel and the relationship and interface with the ISCB. This role may be an authorised ISO/IEC 17025 signatory.

b) **Senior Evaluator/ Senior MTPS Certifier** – This role is responsible for:

i) Ensuring the effective application of IT security evaluation criteria for evaluations conducted within the Security Evaluation Facility;

ii) The technical development of evaluators in the facility;

iii) The continuous application of the facility management system to the conduct of evaluations within the Security Evaluation Facility; and

iv) Acting as an ISO/IEC 17025 authorised signatory for evaluation work.

c) **Evaluator/ MTPS Certifier** – This role is responsible for the conduct of day-to-day evaluation projects under the direction of the Senior Evaluator and in compliance with the facility management system.

d) **SEF Quality Manager** – This role is responsible for maintenance of the facility management system, and conducts reviews of the management system application within the Security Evaluation Facility.

72 The details of licensed Security Evaluation Facilities, including contact information and their status can be found at the respective certification schemes website as stated in Section 2.4 of this document.

73 The detail requirements for Security Evaluation Facilities operations and how to apply to become ISCB licensed Security Evaluation Facilities are described in ISCB Evaluation Facility Manual (ISCB_EFM) (Ref [14]).

# 4 ISCB Product Certification Schemes Rules

## 4.1 General

### 4.1.1 Conflict of Interest

74 ISCB personnel and the Security Evaluation Facilities personnel who are involved in the certification project, shall not be assigned to a certification project under the ISCB product certification schemes if they have a perceived or actual conflict of interest in the outcome.

75 A perceived or real conflict of interest may arise for reasons including:

a) They have been involved in the supply or design of products of the type certified;

b) They have been employed with or by the client organisation;

c) They have given advice or provided consultancy services to the client organisation of a certification project on matters which are barriers to the certification; and/or

d) They have provided any other products or services which could compromise the confidentiality, objectivity or impartiality of certification processes and decisions;

within the last two (2) years.

76 ISCB personnel shall sign a declaration of no conflict of interest prior to their commencement:

a) in any role within ISCB and then every two (2) years, and

b) on each and every certification project.

### 4.1.2 Subcontracting Certification

77 ISCB shall not subcontract the certification decision process.

78 CCRA (Ref [1]) requires that there be only one government entity operating an ICT security certification and evaluation scheme for a certificate authorising participant. Therefore, MyCB is the only certification body in Malaysia operating and certifying the results of the MyCC Scheme certification services.

### 4.1.3 Marketing Restrictions

79 ISCB shall market its product certification schemes services separately from other CyberSecurity Malaysia services.

80 ISCB uses the Internet as the main method of promoting its product certification schemes services. The product certification schemes services are published at the respective certification schemes website as stated in Section 2.4 of this document.

81 ISCB licensed Security Evaluation Facilities shall market their related security evaluation services separately from the services offered by their related organisations.

82 Organisations operating as licensed Security Evaluation Facility are not restricted in their operation. However, there is a potential conflict of interest between the activities the Security Evaluation Facility conducts and those activities of the organisation. For example, an organisation cannot market security design services and security evaluation services together with the implication that evaluation will be easier or faster if a client was to sign-up to both.

83 ISCB product certification schemes symbols and trademarks shall be restricted in their use in accordance with Annex C of this document.

84 The Common Criteria mutual recognition certificate and service marks shall be restricted in its use in accordance with Annex E of the CCRA (Ref [1]).

### 4.1.4 Surveillance

85 The Scheme Manager of the respective certification bodies shall ensure ongoing monitoring of the use of certificates, trademarks and claims to ensure that such usage is compliant with ISCB product certification schemes rules and the CCRA (Ref [1], only for MyCC Scheme), and does not bring the ISCB product certification schemes, or its symbols and logos, into disrepute.

### 4.1.5 Confidentiality Provisions

86 Information received or prepared by ISCB is official information and shall be kept confidential when necessary.

Note that some publications such as this document and certification outputs produced by ISCB are public documents. Some of the documents produced by MyCC Scheme have specific information requirements in accordance with the CCRA (Ref [1]).

87 The confidentiality requirements between ISCB, Security Evaluation Facility, and any organisation may be specified in a confidentiality agreement between two or more parties to a certification project. Confidentiality requirements should include the measures to be used for the storage and transmission of information between the parties to the agreement.

88 ISCB personnel shall sign a confidentiality undertaking prior to their commencement in any role within ISCB.

89 Security Evaluation Facility personnel shall sign a confidentiality undertaking prior to their commencement in any role within their organisation.

### 4.1.6 Client Information Collection

90 ISCB shall ensure the security and confidentiality of the client organisation records, including the following information:

a) Application information and certification documents unless required to be published by the certification scheme such as MyCC Scheme Certification Report and Security Target;

b) Certification/service agreement;

c) Justification of the methodology used for sampling;

d) Justification for certifier/ operator time determination;

e) Verification of non-conformities;

f) Records of complaints and appeals, and any subsequent correction or corrective actions;

g) Committee/management deliberations and decisions, if applicable;

h) Documentation of the certification decisions; and

i) Related records necessary to establish the credibility of the certification, such as evidence of the competence of auditors and technical experts.

### 4.1.7 Client Information Exchange

91 ISCB personnel shall provide and update client organisations on the following:

a) A detailed description of the initial and continuing ISCB product certification schemes activities, including the Accept, Execute/Oversight and Certify functions, and the process for granting, maintaining, and withdrawing certification (if any);

b) The normative requirements for ISCB product certification schemes certification;

c) Information about ISCB product certification schemes fees (if any);

d) The ISCB product certification schemes requirements for prospective clients:

i) To comply with certification schemes requirements;

ii) To make all necessary arrangements for the conduct of the evaluations, including provision for examining documentation and the access to all processes and areas, records and personnel for the purposes of the certification and resolution of complaints; and

iii) To make provisions, where applicable, to accommodate the presence of observers (e.g. accreditation assessors);

e) Documents describing the rights and duties of certified client, including requirements, when making reference to its product certification schemes certification in communications of any kind; and

f) Information on procedures for the handling of ISCB product certification schemes complaints and appeals.

92 ISCB shall provide its certified client due notice of any changes to its product certification schemes requirements for certification and verify that each certified client complies with the new requirements.

93 ISCB shall endure legally enforceable arrangements to ensure that the certified client inform the certification body, without delay, of matters that may affect its ability to conform with the product certification scheme requirements such as:

a) The certified product availability, release, and vulnerability that may affect compliance with the requirements of the certification scheme; and

b) The capability of the management system or organisation's e-business to continue to fulfil the requirements of the standard used for certification.

This include, for example:

a) Changes relating to the legal, commercial, organisational status or ownership;

b) Changes relating to the organisation and management (e.g. key managerial, decision-making or technical staff);

c) Changes relating to their contact details and sites. This is to ensure that the certification register is current;

d) Major changes to the quality management system;

e) There is a firm decision to cease sales and/or technical support of their certified product; and/or

f) They become aware of an exploitable vulnerability in their certified product.

### 4.1.8 Disputes, Complaints and Appeals

94 ISCB shall treat any dispute between ISCB and any party with respect to compliance with ISCB product certification schemes rules or interpretations as a complaint. A disputes, complaints and appeals procedure is published on respective certification schemes website as stated in Section 2.4 of this document and shall be used for reporting, recording and resolving complaints.

95 Any disputes between other parties' e.g. contractual issues between a Security Evaluation Facility and its client shall not be taken as a dispute or complaint with ISCB.

96 The ISCB Head of Department shall ensure that any disputes, complaints and appeals received are fully investigated, documented and appropriate follow-up action taken within ten (10) business days.

97 Any ISCB personnel (including management) that have been involved in activities with the applicant or supplier in question or anybody related to the supplier within the last two years, shall not be involved in investigating any dispute, complaint or appeal.

98 Any decision made by ISCB may be appealed within seven (7) business days of the original decision. An appeals procedure shall be used for making, recording and resolving all appeals. The Head of ISCB Department is responsible for reviewing the original decision and, within ten (10) business days of lodgement, either:

a) Upholding the appeal and publishing a revised decision; or

b) Rejecting the appeal and confirming the original decision as final in which case no further appeals on that decision shall be considered.

## 4.2 ISCB Certification Schemes Process

### 4.2.1 Overview

99 ISCB provides product certification schemes services as described in Section 2.4 of this document. To support the certification services, ISCB provide other services as described in Section 2.5 of this document.

100 In general, certification process consist of three (3) functions as illustrated in Figure 3 below.

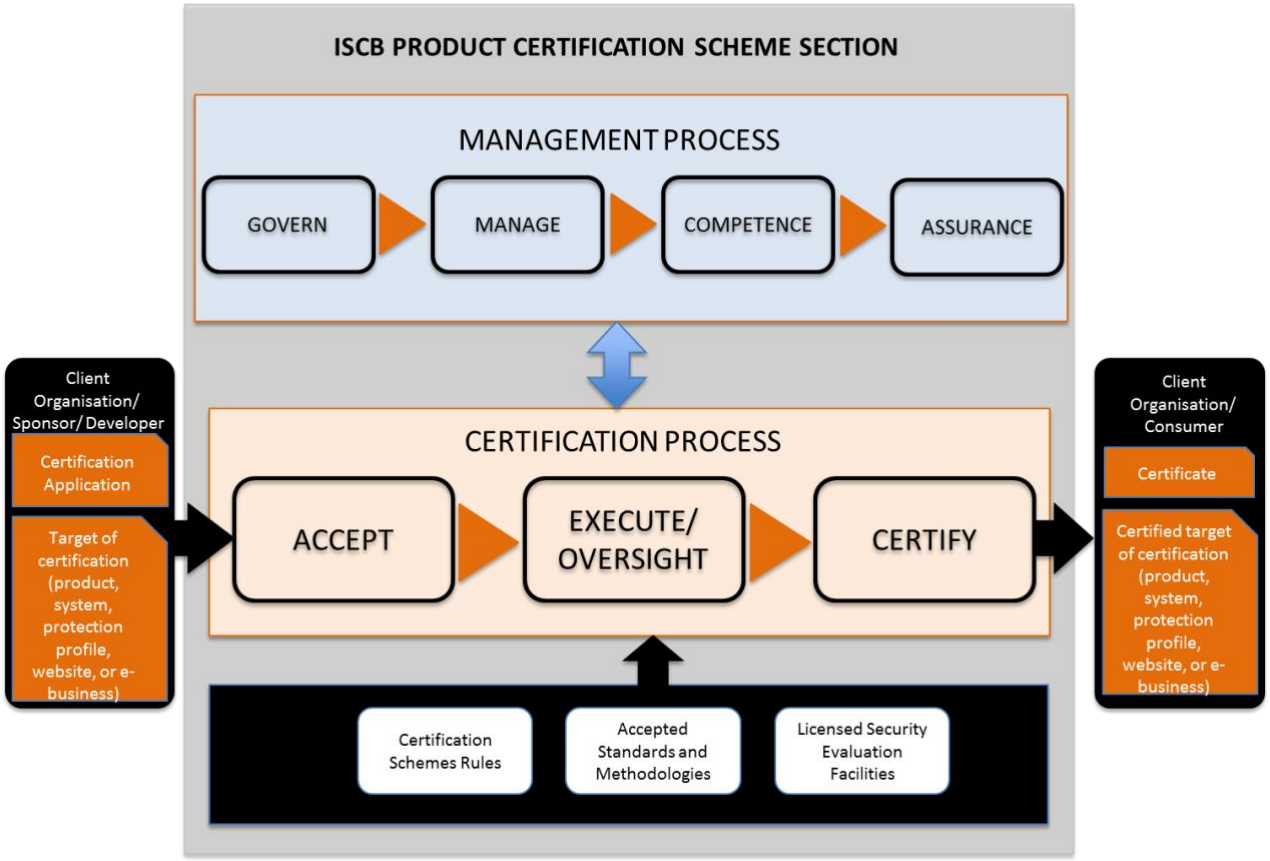


Figure 3: ISCB Product Certification Schemes Process Overview

The functions are:

a) **ACCEPT** – this function that formally accepts (or rejects) a certification application and allocates certification resources.

b) **EXECUTE/OVERSIGHT** – the function that provides continuous oversight of the work performed in evaluating the scope of the certification to gain assurance that the certification scheme rules and approved methodology have been correctly applied.

c) **CERTIFY** – the function for certifying the results of the certification project.

Due to the difference in the certification process and standard requirements of each product certification scheme, the detail of each certification process are documented separately in:

a) MyCC Scheme Certification Process (MyCC_CP) (Ref [15]),

b) MTPS Certification Process (MTPS_CP) (Ref [16]),

c) TSA Scheme Certification Process (TSA_CP) (Ref [17]),

d) MyCMVP Certification Process (MyCMVP_CP) (under development), and

e) MyTrustSEAL Scheme Certification Process (MTSEAL_CP) (under development).

101 ISCB shall also ensure the delivery of its product certification schemes is undertaken in a manner encapsulating good governance, management and administration, high competence, and assurance processes. These processes are described in ISCB Product Certification Manual (PRODUCT_CM) (Ref [13]).

102 However, the documents above are not publicly available. Interested parties seeking access to documents that are not publicly available must submit a request in writing to the ISCB Head of Department. The decision to release these documents to a third party is at the discretion of ISCB and may be subject to conditions as part of that release.

# Annex A Reference Materials

## *A.1 References*

[1] Arrangement on the recognition of Common Criteria Certificates in the field of Information Technology Security, July 2014.

[2] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, CCMB-2009-07-001, Version 3.1, Revision 4, September 2012.

[3] Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, CCMB-2009-07-002, Version 3.1, Revision 4, September 2012.

[4] Common Criteria for Information Technology Security Evaluation, Part 3: Security assessment components, CCMB-2009-07-003, Version 3.1, Revision 4, September 2012.

[5] Common Evaluation Methodology for Information Technology Security Evaluation, CCMB-2009-07-004, Version 3.1, Revision 4, September 2012.

[6] ISO/IEC 19790:2012 – Information technology – Security techniques – Security requirements for cryptographic modules, International Standards Organisation, 2012.

[7] ISO/IEC 24759:2014 – Information technology – Security techniques – Test requirements for cryptographic modules, International Standards Organisation, 2014.

[8] World Trustmark Alliance (WTA) Code of Conduct.

[9] ISO/IEC 17065:2012 – Conformity assessment – Requirements for bodies certifying products, processes and services, International Standards Organisation, 2012.

[10] ISO/IEC 17025:2005 – The General requirements for the Competence of Testing and Calibration Laboratories, International Standards Organisation, 2005.

[11] Latest version of ISCB Product Certification Quality and Security Manual (PRODUCT_QSM) as listed in the ISCB Master Register.

[12] Latest version of ISCB Product Certification Procedures Manual (PRODUCT_PM) as listed in the ISCB Master Register.

[13] Latest version of ISCB Product Certification Manual (PRODUCT_CM) as listed in the ISCB Master Register.

[14] Latest version of ISCB Evaluation Facility Manual (ISCB_EFM) as listed in the ISCB Master Register.

[15] Latest version of MyCC Scheme Certification Process (MyCC_CP) as listed in the ISCB Master Register.

[16] Latest version of MTPS Certification Process (MTPS_CP) as listed in the ISCB Master Register.

[17] Latest version of TSA Scheme Certification Process (TSA_CP) as listed in the ISCB Master Register.

[18] Terms and conditions governing the use of the ACB symbol or reference to STANDARDS MALAYSIA accreditation by Certification Bodies, ACB 2 issue 2 15 February 2007 (Amd.2, 18 April 2012), Department of Standards Malaysia Scheme for the Accreditation of Certification Bodies (The ACB Scheme).

[19] Terms and conditions governing STANDARDS MALAYSIA accredited Certification Bodies on claims of equivalence of accreditation and use of IAF MLA mark, ACB 3 issue 4 1 April 2016 (Amd.1, 3 May 2016), Department of Standards Malaysia Scheme for the Accreditation of Certification Bodies (The ACB Scheme).

## *A.2 Acronyms*

Table 1: List of Acronyms

| Acronyms | Expanded Term |
|---|---|
| ACB | Accreditation of Certification Body |
| CB | Certification Body |
| CC | Common Criteria |
| CEM | Common Evaluation Methodology |
| CCRA | Common Criteria Recognition Arrangement |
| CNII | Critical National Information Infrastructure |
| CPR | Certified Products Register |
| CVF | Cryptography Validation Facility |
| ICT | Information and Communications Technology |
| IEC | International Electrotechnical Commission |
| ISCB | Information Security Certification Body |
| ISCB_EFM | ISCB Evaluation Facility Manual |
| ISMB | ISCB Scheme Management Board |
| ISO | International Standards Organisation |
| MTC | Malaysia Trustmark Certifier |
| MTO | Malaysia Trustmark Operator |

| | |
|---|---|
| MTPS | Malaysia Trustmark for Private Sector |
| MTPS_VWR | MTPS Validated Website Register |
| MTSEAL | MyTrustSEAL Scheme |
| MTSEAL_CB | MTSEAL Certification Body |
| MTSEAL_CWR | MTSEAL Scheme Certified Website Register |
| MyCB | Malaysian Common Criteria Certification Body |
| MyCC | Malaysian Common Criteria Evaluation and Certification |
| MyCMVP | Cryptographic Module Validation Program |
| MyCPR | MyCC Scheme Certified Products Register |
| MySEF | Malaysian Security Evaluation Facility |
| NCSP | National Cyber Security Policy |
| PP | Protection Profile |
| PRODUCT_QSM | ISCB Product Certification Quality and Security Manual |
| PRODUCT_PM | ISCB Product Certification Procedure Manual |
| SPA | Security Posture Assessment |
| SPAF | Security Posture Assessment Facility |
| ST | Security Target |
| TOE | Target of Evaluation |
| TSA | Technology Security Evaluation |
| TSACB | Technology Security Evaluation Certification Body |
| TSA_CPR | TSA Scheme Certified Products Register |
| TSA_MSFR | TSA Mandatory Security Functions Requirement |

## *A.3 Glossary of Terms*

Table 2: Glossary of Terms

| Term | Definition and Source |
|---|---|
| Audit | An assessment of a client organisation's certification scope (e.g. ISMS or MTPS scope) as defined by the certification scheme, proposed by an application against the standards covered by the scope defined in its application against the certification criteria specified in the rules of the certification scheme. |
| Certificate | The official representation from the Certification Body of the certification of a specific version of the recognise certification standards such as ISO/IEC 27001, Common Criteria etc. |
| Certification Body | An organisation responsible for carrying out certification and for overseeing the day-to-day operation of a certification scheme. |
| Certification Scheme | The systematic organisation of the evaluation, audit and certification functions under the authority of a certification body in order to ensure that high standards of competence and impartiality are maintained and that consistency is achieved. |
| Consumer | The organisation that uses the certified product within their infrastructure. |
| Customer/ Client/ Organisation | The organisation (sponsors, developers or consumers) that submits an application and make use of services provided by the ISCB. |
| Developer | The organisation that develops the product submitted for evaluation and certification. |
| Evaluation/ Assessment | The assessment of an IT product, IT system, or any other valid target as defined by ISCB product certification schemes, proposed by an applicant against the standards covered by the scope defined in its application against the certification criteria specified in the ISCB product certification schemes rules. |
| Interpretation | Expert technical judgement, when required, regarding the meaning or method of applicant of any technical aspect of the criteria or the methodology. An |

| | |
|---|---|
| | interpretation may be either a national or international interpretation. |
| ISCB Personnel | Includes all members of the Scheme Manager, Auditor, Certifier, MTPS Operator, Quality Manager, and Head of Department. |
| Lead Certifier | The Certifier responsible for managing a specific certification task. |
| Lead Evaluator | The Evaluator responsible for managing the technical aspects of a specific evaluation task. |
| MTPS Certifier | The personnel responsible for reviewing and assessing the technical and security aspects of the organisation e-business web portal and online payment system. MTPS Certifier is the member of Security Evaluation Facility. |
| MTPS Operator | The personnel responsible for managing the audit and validation project. Auditing of the organisation's MTPS scope is based on the MTPS technical requirements. MTPS Operator is the member of ISCB personnel. |
| Security Evaluation Facility | An organisation (or business unit of an organisation) licensed by ISB that conducts:<br>a) Malaysian Security Evaluation Facility (MySEF) – evaluation facility that is licensed by ISCB to conduct security evaluations of ICT products, systems, and protection profiles against CC and CEM;<br>b) Cryptography Validation Facility (CVF) – evaluation facility that is licensed by ISCB to conduct cryptography conformance and randomness testing against ISO/IEC 19790 and ISO/IEC 24759;<br>c) Security Posture Assessment Facility (SPAF) – organisation or facility that is recognised by ISCB to deliver security posture assessment (SPA) of the certified ICT product operational environment; and<br>d) Malaysia Trustmark Certifier (MTC) – organisation or facility that is recognised by ISCB to conduct Trustmark Technical Security Assessment (TTSA) or to validate the security aspects of the e-business web portal and online payment system against the MTPS technical requirements and additional adopted standards such as PCI-DSS and web security best practices (OWASP). |

| | |
|---|---|
| | Note. The security evaluation facilities above may be provided by the same organisation. |
| Sponsor | The organisation that submits a product for evaluation and certification under the ISCB product certification schemes. The sponsor may also be the developer. |
| Surveillance/ Maintenance of Certificate | The update of certificate to reflect that the certification scope is being maintained under the certification scheme. |

# Annex B ISCB Product Certification Schemes Certification and Service Marks

## *B.1 Purpose*

103 ISCB shall exercise the control as specified by its certification schemes over ownership, use and display of license, certificates, marks of conformity, and any other mechanisms for indicating a product, system, protection profile, or e-business is certified.

104 The purpose of this Annex is to describe general requirement on how ISCB product certification schemes certification and service marks maybe used and referred to by other parties.

105 The details of the specific product certification scheme certification and service marks are published at the respective product certification schemes website as stated in Section 2.4 of this document. It can also be found in the respective certification process document as specified in paragraph 100.

## *B.2 Policy*

106 Any ISCB product certification schemes certification and service marks, and accompanying text authorised for use by ISCB certified products shall:

a) Be traceability back to ISCB;

b) Contain no ambiguity;

i) As what had been certified; and

ii) Which certification body has granted the certification;

c) Not be used in any other way that may be interpreted as denoting different type of certification. For example, process certification mark shall not be used on a product or product packaging seen by the consumer or in any other way that may be interpreted as denoting product conformity.

107 It is incumbent for ISCB to take appropriate administrative, procedural or legal steps to prevent or counter the misuse of certificates and to correct false, misleading or improper statements about certificates or about the product certification schemes operated by ISCB.

108 Upon receipt of a certificate from ISCB, the marks may be used by the organisation or individual in conjunction with advertising, marketing, and sales for which the certificate is issued. ISCB shall make necessary legal arrangements with the client organisations, to the effect that they are required to:

a) use the issued certificate in documentation or marketing material by reproducing the entire certificate in an accurate and readable form;

b) conform to the requirements of the product certification scheme rules and requirement when making reference to its certification status in communication media such as the internet, brochures or advertising, or other documents;

c) not make or permit any misleading statement regarding its certification;

d) not use or permit the use of a certification document or any part thereof in a misleading manner;

e) upon suspension, withdrawal or termination of its certification, discontinues its use of all advertising matter that contains a reference to certification, as directed by ISCB;

f) not allow reference to its certification to be used in such a way as to either express or imply that CyberSecurity Malaysia, the certification scheme, or other organisation that recognises or gives effect to this certificate, endorse or give warranty to the certified product;

g) not imply that the certification applies to activities that are outside the scope of certification; and

h) not use its certification in such a manner that would bring CyberSecurity Malaysia and the product certification scheme into disrepute and lose public trust.

## *B.3 CCRA Certification Mark*

109 A product whose certificate is recognised by MyCC Scheme and CCRA may carry the CCRA Certification mark, under conditions as outlined in CCRA Annex E Certificate and Service Marks (Ref [1]). This mark confirms that the Common Criteria certificate has been authorised by a CCRA Participant.

## *B.4 Accreditation Mark*

110 Certification Bodies accredited by Jabatan Standards Malaysia, the Malaysian accreditation body, are given the right to use an Accreditation Symbol in accordance with ACB 2 (Ref [18]) and ACB 3 (Ref [19]).

## *B.5 Misuse of the ISCB Product Certification and Service Mark*

111 ISCB shall monitor the use of its product certification and service mark.

112 In order to respond to a reported misuse of ISCB product certification and service mark, a number of factors are considered such as:

a) the laws of the country in which the misuse occurs,

b) the nature of the contract or agreement between the certification body and the party misusing the mark,

c) the seriousness of the misuse,

d) whether the misuse was inadvertent or deliberate, or

e) whether the certified product, process or professional is harmful.

113 ISCB shall investigate any report regarding to the misuse of its product certification and service mark.

114 Incorrect references to ISCB product certification schemes, or misleading use of license, certificates, marks, and any other mechanism for indicating a product, process or professional is certified, found in documentation or other publicity, shall be dealt with by suitable action such as corrective actions, withdrawal of certificate, publication of the transgression and, if necessary, legal action.

--- END OF DOCUMENT ---