C137 Certification Report

Pradotec BioCard v1.0

File name: ISCB-5-RPT-C137-CR-v1a
Version: v1a
Date of document: 5 November 2024
Document classification: PUBLIC

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

C137 Certification Report

Pradotec BioCard v1.0

5 November 2024

ISCB Department

CyberSecurity Malaysia

Level 7, Tower 1,
Menara Cyber Axis, Jalan Impact,
63000 Cyberjaya, Selangor, Malaysia
Tel: +603 8800 7999 □ Fax: +603 8008 7000
http://www.cybersecurity.my

Document Authorisation

DOCUMENT TITLE:	C137 Certification Report
DOCUMENT REFERENCE:	ISCB-5-RPT-C137-CR-v1a
ISSUE:	v1a
DATE:	5 November 2024
DISTRIBUTION:	UNCONTROLLED COPY - FOR UNLIMITED USE AND DISTRIBUTION

Copyright Statement

Registered office:

Level 7, Tower 1

Menara Cyber Axis

Jalan Impact

63000 Cyberjaya

Selangor Malaysia

Registered in Malaysia – Company Limited by Guarantee

Company No. 201601006881 (726630-U)

Printed in Malaysia

Foreword

The Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme has been established under the 9th Malaysian Plan to increase Malaysia's competitiveness in quality assurance of information security based on the Common Criteria (CC) standard and to build consumers' confidence towards Malaysian information security products.

The MyCC Scheme is operated by CyberSecurity Malaysia and provides a model for licensed Malaysian Security Evaluation Facilities (MySEFs) to conduct security evaluations of ICT products, systems and protection profiles against internationally recognised standards. The results of these evaluations are certified by the Malaysian Common Criteria Certification Body (MyCB) Unit, a unit established within Information Security Certification Body (ISCB) Department, CyberSecurity Malaysia.

By awarding a Common Criteria certificate, the MyCB asserts that the product complies with the security requirements specified in the associated Security Target. A Security Target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the Security Target, in addition to this certification report, to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product satisfies the security requirements.

This certification report is associated with the certificate of product evaluation dated 7 November 2024 and the Security Target (Ref [6])The certification report, Certificate of product evaluation and security target are posted on the MyCC Scheme Certified Product Register (MyCPR) at MyCC under ISCB Website and the Common Criteria Portal (the official website of the Common Criteria Recognition Arrangement).

Reproduction of this report is authorised provided the report is reproduced in its entirety.

Disclaimer

The Information Technology (IT) product identified in this certification report and its associate certificate has been evaluated at an accredited and licensed evaluation facility established under the Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme using the Common Methodology for IT Security Evaluation, version 3.1 revision 5 (Ref [3]), for conformance to the Common Criteria for IT Security Evaluation, version 3.1 revision 5 (Ref [2]). This certification report and its associated certificate apply only to the specific version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the MyCC Scheme and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certification report and its associated certificate is not an endorsement of the IT product by CyberSecurity Malaysia or by any other organisation that recognises or gives effect to this certification report and its associated certificate, and no warranty of the IT product by CyberSecurity Malaysia or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Document Change Log

RELEASE	DATE	PAGES AFFECTED	REMARKS/CHANGE REFERENCE
d1	9 Oct 2024	All	Initial draft
d1a	18 Oct 2024	1,8,9	Updated based on comments from reviewers
v1	28 Oct 2024	All	Final Version
v1a	5 Nov 2024	4	Updated based on SCC's comment – add hardware and SDK version

Executive Summary

The Target of Evaluation (TOE) is Pradotec BioCard v1.0, designed as an efficient and secure smart card reader with integrated biometric capabilities, comprises several essential components that work together to facilitate Malaysian Identity Card (MyKad, MyKid, MyTentera, MyPolis and MyPR cards) verification processes. The TOE is essentially a wired biometric smart card reader designed specifically for reading Malaysian Identity Cards and perform thumbprint verification process. The TOE comprises of two key components which are Pradotec BioCard Hardware Device (PRADOTECBIOCARD-DEVICE) and Pradotec BioCard Web Based SDK (PRADOTECBIOCARD-SDK). The security features of the TOE included in the evaluation are Identity Verification and Protection of TSF.

The scope of the evaluation is defined by the Security Target (Ref[6]) which identifies security objectives for the environment, the security functional requirements, and the evaluation assurance level at which the product is intended to satisfy the security requirements. Prospective consumers are advised to verify that their operating environment is consistent with the evaluated configuration, and to give due consideration to the comments, observations and recommendations in this certification report.

This report confirms the findings of the security evaluation of the TOE to the Common Criteria (CC) Evaluation Assurance Level 1 (EAL1). This report confirms that the evaluation was conducted in accordance with the relevant criteria and the requirements of the Malaysia Common Criteria Evaluation and Certification (MyCC) Scheme (Ref [4]).

The evaluation was performed by CyberSecurity Malaysia MySEF (CSM MySEF) and the evaluation was completed on 8 October 2024.

The Malaysia Common Criteria Certification Body (MyCB), as the MyCC Scheme Certification Body, declares that the TOE evaluation meets all the Arrangements on the Recognition of Common Criteria certificates and the product will be listed in the MyCC Scheme Certified Products Register (MyCPR) and the Common Criteria portal (the official website of the Common Criteria Recognition Arrangement) at http://www.commoncriteriaportal.org

It is the responsibility of the user to ensure that Pradotec BioCard v1.0 meets their requirements. It is recommended that a potential user of the TOE refer to the Security Target (Ref [6]) and this Certification Report prior to deciding whether to purchase the product.

Table of Contents

Index of Tables

Index of Figures

1 Target of Evaluation

1.1 TOE Description

1 The Target of Evaluation (TOE) is Pradotec BioCard v1.0. The TOE is designed by Pradotec Sales & Services Sdn Bhd, serves as a wired biometric smart card reader, specifically crafted to cater to the verification needs of Malaysian Identity Cards (MyKad, MyKid, MyTentera, MyPolis and MyPR cards). However, MyKid card does not have stored fingerprint templates and thus it is unable to undergo fingerprint verification. This device aims to streamline over-the-counter biometric processes, offering a seamless user experience and robust security measures.

2 This product was developed with the main purpose to provide a secure and efficient solution for Malaysian Identity Cards verification. The TOE designed as an efficient and secure smart card reader with integrated biometric capabilities, comprises several essential components that work together to facilitate Malaysian Identity Card verification processes.

3 Below are the key components of the TOE:

1. Pradotec BioCard Hardware Device (PRADOTECBIOCARD-DEVICE)

   This is a compact biometric smart card reader designed for seamless identity verification. The design has a slot for Malaysia Identity Cards and an integrated thumbprint sensor by connecting to a laptop or PC via wired USB. Users can read Malaysian Identity Cards' data or opt for advanced verification by scanning their thumbprint, ensuring robust identity verification. Its user-friendly interface and design make it as solution for businesses seeking secure, over-the-counter biometric processes.

   a) **Smart Card Slot:** The Pradotec BioCard Hardware Device features a dedicated slot designed to accommodate various Malaysian Identity Cards. This slot allows the insertion of the respective Malaysian Identity Cards for data reading and processing.

   b) **Thumbprint Sensor:** An integral component of the Pradotec BioCard Hardware Device, the thumbprint sensor enables thumbprint verification. It captures and processes thumbprint data for verification purposes, ensuring that the individual using the Malaysian Identity Card (excluding MyKid) is the authorized owner.

c) **Wired Connectivity:** The Pradotec BioCard Hardware Device is equipped with wired connectivity, typically using a USB interface, enabling seamless connection to desktops or laptops. This connectivity facilitates data transmission between the Pradotec BioCard and the connected device running the SDK for further processing and verification.

d) **Integrated Circuitry:** The internal circuitry within the Pradotec BioCard Hardware Device processes the data retrieved from the Malaysian Identity Card and the thumbprint sensor. It manages the interaction between the various components and perform user's thumbprint verification with Malaysian Identity Cards.

2. Pradotec BioCard Web Based SDK (PRADOTECBIOCARD-SDK)

While not a physical component of the Pradotec BioCard itself, the SDK provided by Pradotec is an essential component of the ecosystem. This kit enables developers to create customized applications that leverage the Pradotec BioCard's functionalities for data verification, extraction, and other operations necessary for identity verification processes.

4 The following list highlights the range of security functions implemented by the TOE:

I. Identity Verification

II. Protection of TSF

1.2 TOE Identification

5 The details of the TOE are identified in Table 1: TOE Identification below.

Table 1: TOE Identification

Evaluation Scheme	Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme
Project Identifier	C137
TOE Name	Pradotec BioCard
TOE Version	v1.0
Security Target Title	Pradotec BioCard v1.0 Security Target
Security Target Version	1.0
Security Target Date	6 August 2024

Assurance Level	Evaluation Assurance Level 1
Criteria	Common Criteria for Information Technology Security Evaluation, April 2017, Version 3.1, Revision 5 (Ref [2])
Methodology	Common Methodology for Information Technology Security Evaluation, April 2017, Version 3.1, Revision 5 (Ref [3])
Protection Profile Conformance	None
Common Criteria Conformance	CC Part 2 Conformant CC Part 3 Conformant Package conformant to EAL 1
Sponsor	Pradotec Sales & Services Sdn Bhd Bukit Jalil City Signature Shop-Office, N1-2, Pusat Perdagangan Bandar Bukit Jalil, Persiaran Jalil 3, 57000 Kuala Lumpur.
Developer	Pradotec Sales & Services Sdn Bhd Bukit Jalil City Signature Shop-Office, N1-2, Pusat Perdagangan Bandar Bukit Jalil, Persiaran Jalil 3, 57000 Kuala Lumpur.
Evaluation Facility	CyberSecurity Malaysia MySEF (CSM MySEF) Level 7, Tower 1 Menara Cyber Axis Jalan Impact 63000 Cyberjaya Selangor Malaysia

1.3 Security Policy

6 There is no organisational security policy defined regarding the use of TOE.

1.4 TOE Architecture

7 The TOE consist of logical and physical boundaries which are described in Section 1.6 of the Security Target (Ref [6]).

1.4.1 Logical Boundaries

8 The logical boundary of the TOE is summarized below.

- Identity Verification

The TOE verification process integrates Malaysian Identity Card reading and thumbprint verification. Upon insertion of a Malaysian Identity Card into the dedicated slot, the device initiates a data retrieval sequence, extracting and validating card information. Simultaneously, the integrated thumbprint sensor captures the user's thumbprint data and compares it against the stored template within a secure enclave. If identity verification is requested, the Pradotec BioCard prompts the individual to place their thumb on the sensor, initiating a biometric match process that validates the presented thumbprint against the stored data, confirming the cardholder's identity.

- Protection of TSF

The TOE implements robust protection of its TOE Security Functions (TSF) through the strategic deployment of tamper-evident labels, a physical security measure integrated into the device's design. These labels, meticulously placed across critical access points and sensitive areas of the Pradotec BioCard casing, consist of specialized materials or designs engineered to reveal visible indications of interference or attempted intrusion. Their primary purpose is to serve as a barrier against unauthorized access or tampering. Once the tamper-evident labels are disturbed or removed, they irreversibly reveal visible signs of tampering, such as altered patterns, visible markings, or damage, enabling immediate identification of potential security breaches and necessitating further investigation or intervention by user to maintain the device's integrity and security posture.

1.4.2 Physical Boundaries

9 The implementation of the TOE can be found in Figure 1 below. The TOE consists of two main components:

- PRADOTECBIOCARD-DEVICE: Pradotec BioCard Hardware Device v0596 and
- PRADOTECBIOCARD-SDK: Pradotec BioCard Web-based Software Development Kits v1.2.x.x**

**Note: x.x represent (Build Number.Revision Number)

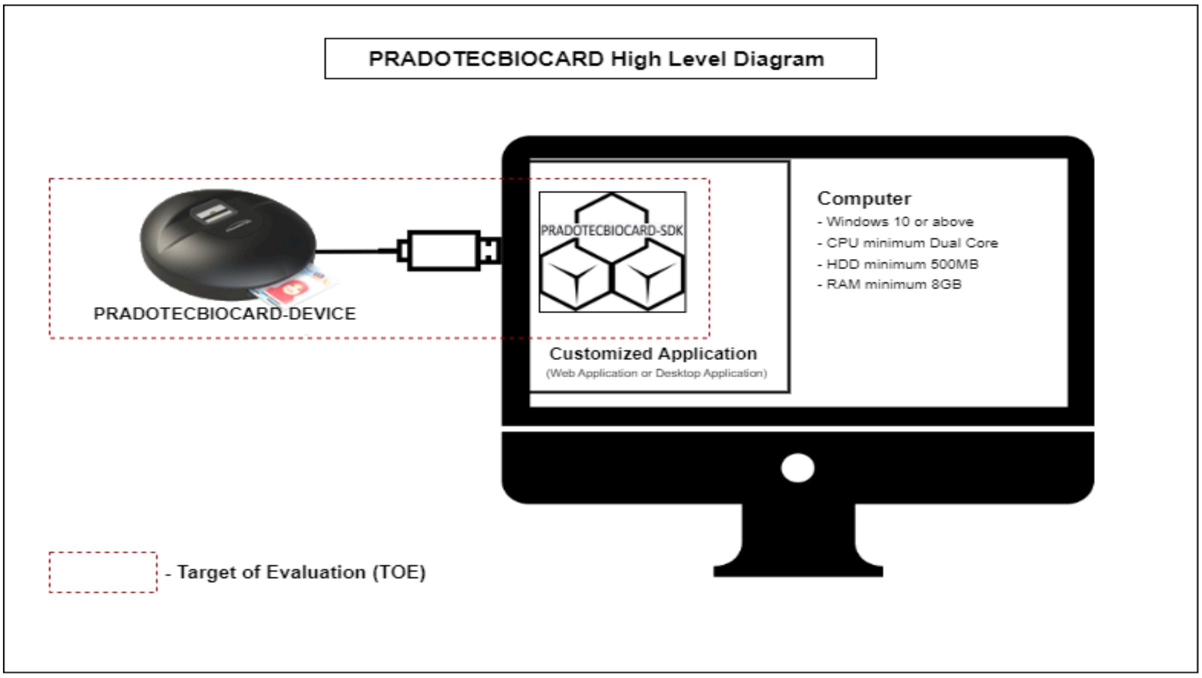

Figure 1 – Implementation of TOE

10 Figure 1 shows the environment where the TOE components carry out its operation. PRADOTECBIOCARD-DEVICE connects to a laptop or PC via USB and enables thumbprint verification. PRADOTECBIOCARD-SDK allows developers to create customized applications that leverage the PRADOTECBIOCARD-DEVICE's functionalities.

11 Each of these components plays a crucial role in the Pradotec BioCard's ability to read and process data from Malaysian Identity Cards, perform thumbprint verification, and transmit the verification result for data processing through the connected software applications via PRADOTECBIOCARD-SDK.

1.5 Clarification of Scope

12 The TOE is designed to be suitable for use in accordance with user guidance that is supplied with the product.

13 Section 1.4 of this document describes the scope of the evaluation, which is limited to those claims made in the Security Target (Ref [6]).

14 Potential consumers of the TOE are advised that some functions and services of the overall product have not been evaluated as part of this evaluation. Potential consumers

of the TOE should carefully consider their requirements for using functions and services outside of the evaluated configuration.

1.6 Assumptions

15 There are no assumptions defined regarding the use of TOE.

1.7 Evaluated Configuration

16 This section describes the configurations of the TOE that are included within the scope of the evaluation.

17 As stated in the ST (Ref. [6]) there are two (2) main components that make up the TOE in its evaluated configuration which are PRADOTECBIOCARD-DEVICE and PRADOTECBIOCARD-SDK. PRADOTECBIOCARD-DEVICE comes with the PRADOTECBIOCARD-SDK, which allows users to develop browser-based applications and integrate reading Malaysian Identity Cards.

18 The TOE is configured according to the Guidance documents. The requirement for the environment is as follows:

Hardware:

a) Operating System: Windows 10 and above
b) CPU: Minimum of dual core
c) HDD: Minimum of 500MB
d) RAM: Minimum of 8GB

Software:

a) Microsoft .NET Framework 4.7.2
b) Visual C++ 2013 Runtimes - Microsoft VC++ 2013 x86 Runtimes or Redistributable is required for the PRADOTECBIOCARD-SDK to work fine and will be automatically installed by the installer during the installation.
c) Drivers - For PRADOTECBIOCARD-DEVICE: The PRADOTECBIOCARD-SDK already has the relevant drivers required for running the PRADOTECBIOCARD-SDK using PRADOTECBIOCARD-DEVICE. The installer will install the required drivers during the installation.

19 For evaluation purposes, the testing was conducted using an environment configured according to the baseline defined in the Guidance documents. The detailed configuration used during the testing is as follows:

a. Operating System: Windows 11 Pro

b. CPU: 12th Gen Intel(R) Core (TM) i5-1250P

c. HDD: 500GB

d. RAM: 16GB

1.8 Delivery Procedures

20 The two component of the TOE is delivered separately. The PRADOTECBIOCARD-DEVICE will be sealed in packaging box with security tape, and to be delivered to customer via courier. The PRADOTECBIOCARD-SDK is to be delivered to customers via Google Drive.

21 However, for this EAL1 evaluation, TOE Delivery (ALC_DEL) is not included in the scope of the evaluation. Thus, the evaluator did not verify any TOE delivery process.

2 Evaluation

22 The evaluation was conducted in accordance with the requirements of the Common Criteria, version 3.1 Revision 5 (Ref [2]) and the Common Methodology for IT Security Evaluation (CEM), version 3.1 Revision 5 (Ref [3]). The evaluation was conducted at Evaluation Assurance Level 1. The evaluation was performed conformant to the MyCC Scheme Requirement (MyCC_REQ) (Ref [4]) and ISCB Evaluation Facility Manual (ISCB_EFM) (Ref [5]).

2.1 Evaluation Analysis Activities

23 The evaluation activities involved a structured evaluation of the TOE, including the following components:

2.1.1 Life-cycle support

24 The evaluator found that the TOE provided for evaluation is labelled with its reference.

25 The evaluator examined that the configuration items were clearly and uniquely identifies each configuration item, and it was found to be consistent with the provided evidence.

26 The evaluator confirmed that all the requirements for this class were fulfilled and passed.

2.1.2 Development

27 The evaluator analyzed the TOE functional specification; they examined the functional specification described the purpose and method of use for each SFR-enforcing TOE security functionality interfaces (TSFIs), it identifies all parameters associated with each SFR-enforcing TSFI, and how the TOE security function (TSF) implements the security functional requirements (SFRs).

28 The evaluator determined that the functional specification is accurate and complete instantiation of the SFRs.

29 The evaluator confirmed that all the requirements for this class were fulfilled and passed.

2.1.3 Guidance documents

30 The evaluator examined the TOE preparative user guidance and operational user guidance, and determined that it sufficiently described the security measures to be followed for each user and described all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in order to fulfil the security objectives for the operational environment.

31 The evaluator examined and tested the preparative and operational guidance, and determined that they were complete and sufficiently detailed to result in a secure operation.

32 The evaluator confirmed that the TOE guidance was fulfilled all the requirements and passed for this class.

2.1.4 IT Product Testing

33 Testing at EAL 1 consists of performing independent functional test and conducting penetration tests. The TOE testing was conducted by CyberSecurity Malaysia MySEF (CSM MySEF). The detailed testing activities, including configurations, procedures, test cases, expected results and actual results are documented in a separate Test Plan Report.

2.1.4.1 Independent Functional Testing

34 At EAL 1, independent functional testing is the evaluation conducted by evaluator based on the information gathered by examining design and guidance documentation, examining developer's test documentation, executing a subset of the developer's test plan, and creating test cases that are independent of the developer's tests.

35 All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. The results of the independent functional tests were recorded by the evaluator and are consistent with the expected test results in the test documentation.

Table 2: Independent Functional Test

Test Title	Description	Security Function	TSFI	Results
Test Group A: Identity Verification				

Test Title	Description	Security Function	TSFI	Results
A.1 Read MyKAD	To test that the TOE successfully read the MyKAD information when inserted into the TOE.	FIA_UID.2	Identity Verification	Passed.
A.2 Read MyKAD and verify fingerprint using right thumb	To test that the TOE successfully read the myKAD information and verify the right thumb against the MyKAD information.			
A.3 Read MyKAD and verify fingerprint using left thumb	To test that the TOE successfully read the myKAD information and verify the left thumb against the MyKAD information.			
A.4 Read MyKid	To test that the TOE successfully read the MyKid information when inserted into the TOE.			
Test Group B: Protection of TSF				
B.1 Verifying tamper-evident label on TOE	To test the TOE implementation on the protection of the TSF through deployment of tamper-evident labels.	FPT_PHP.1	Physical Protection	Passed.

36 All testing performed by evaluator produced the expected results and as such the TOE behaved as expected.

2.1.4.2 Vulnerability Analysis

37 The evaluator performed a vulnerability analysis of the TOE in order to identify potential vulnerabilities in the TOE. This vulnerability analysis considered public domain sources and an analysis of guidance documentation and functional specification.

38 From the vulnerability analysis, the evaluator conducted penetration testing to determine that the TOE is resistant to attack performed by an attacker possessing a basic attack potential. The following factors have been taken into consideration during penetration tests:

a) Time taken to identify and exploit (elapsed time);

b) Specialist technical expertise required (specialised expertise);

c) Knowledge of the TOE design and operation (knowledge of the TOE);

d) Window of opportunity; and

e) IT hardware/software or other equipment required for exploitation.

2.1.4.3 Vulnerability testing

39 The penetration tests focused on:

a) Manipulation of False Fingerprint Verification

b) Breaking physical tamper-evident label

40 The result of the penetration testing noted that there is no residual vulnerability found. However, it is important to ensure that the TOE is use only in its evaluated configuration and in secure environment as specified in the Security Target (Ref [6]).

2.1.4.4 Testing Results

41 Tests conducted for the TOE produced the expected results and demonstrated that the product behaved as specified in its Security Target and its functional specification. Therefore, the certifiers confirmed that all the test conducted were PASSED as expected.

3 Result of the Evaluation

42 After due consideration during the oversight of the execution of the evaluation by the certifiers and of the Evaluation Technical Report (Ref [7]), the Malaysian Common Criteria Certification Body certifies the evaluation of Pradotec BioCard v1.0 which is performed by CyberSecurity Malaysia MySEF (CSM MySEF).

43 CyberSecurity Malaysia MySEF (CSM MySEF) found that Pradotec BioCard v1.0 upholds the claims made in the Security Target (Ref [6]) and supporting documentations and has met the requirements of the Common Criteria (CC) Evaluation Assurance Level 1.

44 Certification is not a guarantee that a TOE is completely free of exploitable vulnerabilities. There will remain a small level of risk that exploitable vulnerabilities remain undiscovered in its claimed security functionality. The risk is reduced as the certified level of assurance increases for the TOE.

3.1 Assurance Level Information

45 EAL 1 provides a basic level of assurance by a limited security target and an analysis of the SFRs in that ST using a functional and interface specification and guidance documentation, to understand the security behaviour.

46 The analysis is supported by a search for potential vulnerabilities in the public domain and independent testing (functional and penetration) of the TSF.

47 EAL 1 also provides assurance through unique identification of the TOE and of the relevant evaluation documents.

48 This EAL provides a meaningful increase in assurance over unevaluated IT.

3.2 Recommendation

49 The Malaysian Certification Body (MyCB) is strongly recommended that:

a) Developer is recommended to enhance the biometric verification accuracy by implementing liveliness detection for the fingerprint verification process.

b) Developer is recommended to keep on updating the TOE user Guide and relevant documentations based on updated features of the TOE.

Annex A References

A.1 References

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

[2] The Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017.

[3] The Common Methodology for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017.

[4] MyCC Scheme Requirement (MYCC_REQ), v1b, CyberSecurity Malaysia, July 2023.

[5] ISCB Evaluation Facility Manual (ISCB_EFM), v3, January 2023.

[6] Pradotec BioCard v1.0 Security Target, Version 1.0, 6 August 2024.

[7] CyberSecurity Malaysia MySEF E054 Pradotec BioCard v1.0 Evaluation Technical Report, v1, 8 October 2024.

A.2 Terminology

A.2.1 Acronyms

Table 3: List of Acronyms

Acronym	Expanded Term
CB	Certification Body
CC	Common Criteria (ISO/IEC15408)
CEM	Common Evaluation Methodology (ISO/IEC 18045)
CCRA	Common Criteria Recognition Arrangement
IEC	International Electrotechnical Commission
ISO	International Organisation for Standardization
ISCB	Information Security Certification Body
MyCB	Malaysian Common Criteria Certification Body

Acronym	Expanded Term
MyCC	Malaysian Common Criteria Evaluation and Certification Scheme
MyCPR	MyCC Scheme Certified Products Register
MySEF	Malaysian Security Evaluation Facility
PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation

A.2.2 Glossary of Terms

Table 4: Glossary of Terms

Term	Definition and Source
CC International Interpretation	An **interpretation** of the CC or CEM issued by the CCMB that is applicable to all CCRA participants.
Certificate	The official representation from the CB of the certification of a specific version of a product to the Common Criteria.
Certification Body	An organisation responsible for carrying out **certification** and for overseeing the day-today operation of an **Evaluation and Certification Scheme**. Source CCRA
Consumer	The organisation that uses the certified product within their infrastructure.
Developer	The organisation that develops the product submitted for CC evaluation and certification.
Evaluation	The assessment of an IT product, IT system, or any other valid target as defined by the scheme, proposed by an applicant against the standards covered by the scope defined in its application against the certification criteria specified in the rules of the scheme. Source CCRA and MS-ISO/IEC Guide 65

Term	Definition and Source
Evaluation and Certification Scheme	The systematic organisation of the functions of **evaluation** and **certification** 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. Source CCRA.
Interpretation	Expert technical judgement, when required, regarding the meaning or method of application of any technical aspect of the criteria or the methodology. An interpretation may be either a **national interpretation** or a **CC international interpretation**.
Certifier	The certifier responsible for managing a specific certification task.
Evaluator	The evaluator responsible for managing the technical aspects of a specific evaluation task.
Maintenance Certificate	The update of a Common Criteria certificate to reflect a specific version of a product that has been maintained under the MyCC Scheme.
National Interpretation	An **interpretation** of the CC, CEM or MyCC Scheme rules that is applicable within the MyCC Scheme only.
Security Evaluation Facility	An organisation (or business unit of an organisation) that conducts ICT security evaluation of products and systems using the CC and CEM in accordance with Evaluation and Certification Scheme policy
Sponsor	The organisation that submits a product for evaluation and certification under the MyCC Scheme. The sponsor may also be the developer.

--- END OF DOCUMENT ---