Ref: PRADOTECBIOCARD-ST-1.0

Pradotec BioCard v1.0 Security Target

DOCUMENT VERSION	**1.0**
DOCUMENT DATE	**06-AUG-2024**

Pradotec Sales & Services Sdn Bhd
Bukit Jalil City Signature Shop-Office, N1-2,
Pusat Perdagangan Bandar Bukit Jalil,
Persiaran Jalil 3, 57000 Kuala Lumpur.
Tel: +6017 6147 486
Website: https://www.pradotec-global.com/

Prepared by:

DOCUMENT REVISION HISTORY

Version No.	Published Date	Description of changes	Author
0.1	05-JAN-2024	First draft release	Wilson Lim
0.2	15-JAN-2024	Terminology update	Wilson Lim
0.3	28-FEB-2024	EOR1 Fixing	Reyes Foong
0.4	06-MAY-2024	EOR3 and EOR4 Fixing	Reyes Foong
0.5	24-MAY-2024	EOR4 and EOR5 Fixing	Reyes Foong
0.6	18-JUL-2024	EOR6 Fixing	Reyes Foong
1.0	06-AUG-2024	Finalized Document	Reyes Foong

TABLE OF CONTENTS

1 Security Target Introduction

1.1 Security Target Reference

Security Target Title:	Pradotec BioCard v1.0 Security Target
Security Target Version:	1.0
Security Target Date:	06-AUG-2024

Table 1 - ST Reference

1.2 TOE Reference

	TOE NAME:	**TOE VERSION:**
TOE Name & Version:	Pradotec BioCard	v1.0
TOE Initial:	PRADOTECBIOCARD	

Table 2 - TOE Reference for Pradotec Biocard

1.3 Terminology and Acronyms

Acronyms	Full Name
PRADOTECBIOCARD-DEVICE	Pradotec BioCard Hardware Device
PRADOTECBIOCARD-SDK	Pradotec BioCard Web Based SDK
SDK	Software Development Kits
CC	Common Criteria
EAL	Evaluation Assurance Level
OSP	Organizational Security Policy
PP	Protection Profile
SAR	Security Assurance Requirements
SFR	Security Functional Requirements
ST	Security Target

TOE	Target of Evaluation
TSF	TOE Security Functionality
TSS	TOE Summary Specification
USB	Universal Serial Bus
Malaysian Identity Cards	MyKad, MyKid, MyTentera, My Polis and MyPR
Customized Applications	Desktop Applications, Web-based applications etc.
Users	Refers to the direct consumer of the TOE, who are developers, that would utilize the PRADOTECBIOCARD-SDK to build customized applications.

Table 3: Terminology and Acronyms

1.4 Product Overview

The Pradotec BioCard, designed by Pradotec, 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). This chic and user-friendly device aims to streamline over-the-counter biometric processes, offering a seamless user experience and robust security measures.

The TOE consists of two major components:

- PRADOTECBIOCARD-DEVICE: Pradotec BioCard Hardware Device and
- PRADOTECBIOCARD-SDK: Pradotec BioCard Web-based Software Development Kits

The versions of both of these components are as below:

Component	Version
PRADOTECBIOCARD-DEVICE	v0596
PRADOTECBIOCARD-SDK	v1.2.x.x

Please refer to

- Table 4: Pradotec BioCard Hardware Device Specification

Type	Specification
Dimension (mm)	• 129mm (L) x 119mm (W) x 33mm (H)
Power Source	• Wired USB 2.0 connection full speed 12Mbps
USB Interface Protocol	• USB CCID
Contact Smart Card Standard	• ACR39U ICC reader standard ISO 7816 Parts 1-4, Class A, B, C (5V, 3V, 1.8V)
Device Driver Operation SystemSupport	• Windows®
Thumbprint Sensor	• IDEMIA CBM V3 Optical Sensor
Malaysian Identity Card Verification Speed	• Approximately 7-9 sec

Certification & Compliance	• ISO 7816 Parts 1-4, Class A, B, C (5V, 3V, 1.8V)

Table 4: Pradotec BioCard Hardware Device Specification

- Table 5: Pradotec BioCard Web-based SDK Specification

Type	Specification
Programming Language	• The Web SDK is language neutral. Any programming language that supports HTTP requests and JSON parsing can be used
Request Format	• All of the requests utilize HTTP GET methods and if there are any parameters they are passed as Query/GET Parameters. None of the requests currently has request body.
Data Transfer/ Response Format	• JSON
Error Handling	• All of the responses will follow standard HTTP Response codes like (200, 400, 404, 500 etc). While most responses could be having HTTP status code 200 – it is essential for the user to look into the JSON data returned by the call to get the accurate information
Web SDK Sample	• HTML /Javascript / JQuery 3.3

Table 5: Pradotec BioCard Web-based SDK Specification

1.5 TOE Overview

TOE Overview summarizes the usage and major security features of the TOE. TOE Overview provides context for the evaluated TOE by identifying the TOE type, describing the product, and defining the specific evaluated configuration.

1.5.1 Usage and Major Security Feature of the TOE

Pradotec BioCard is the product designed and developed by Pradotec Sales & Services Sdn Bhd. This product was developed with the main purpose to provide a secure and efficient solution for Malaysian Identity Cards verification.

The Pradotec BioCard, 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. The TOE comprises of two key components. Below is the breakdown of its key components:

1. **Pradotec BioCard Hardware Device (PRADOTECBIOCARD-DEVICE):** This is a compact and sophisticated biometric smart card reader designed for seamless identity verification. Its sleek design houses a slot for Malaysia Identity Cards and an integrated thumbprint sensor. Connecting to a laptop or PC via USB, this wired device enables efficient thumbprint verification. Users can swiftly read Malaysian Identity Cards' data or opt for advanced verification by scanning their thumbprint, ensuring robust identity verification. Its user-friendly interface and chic design make it an ideal 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.

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.

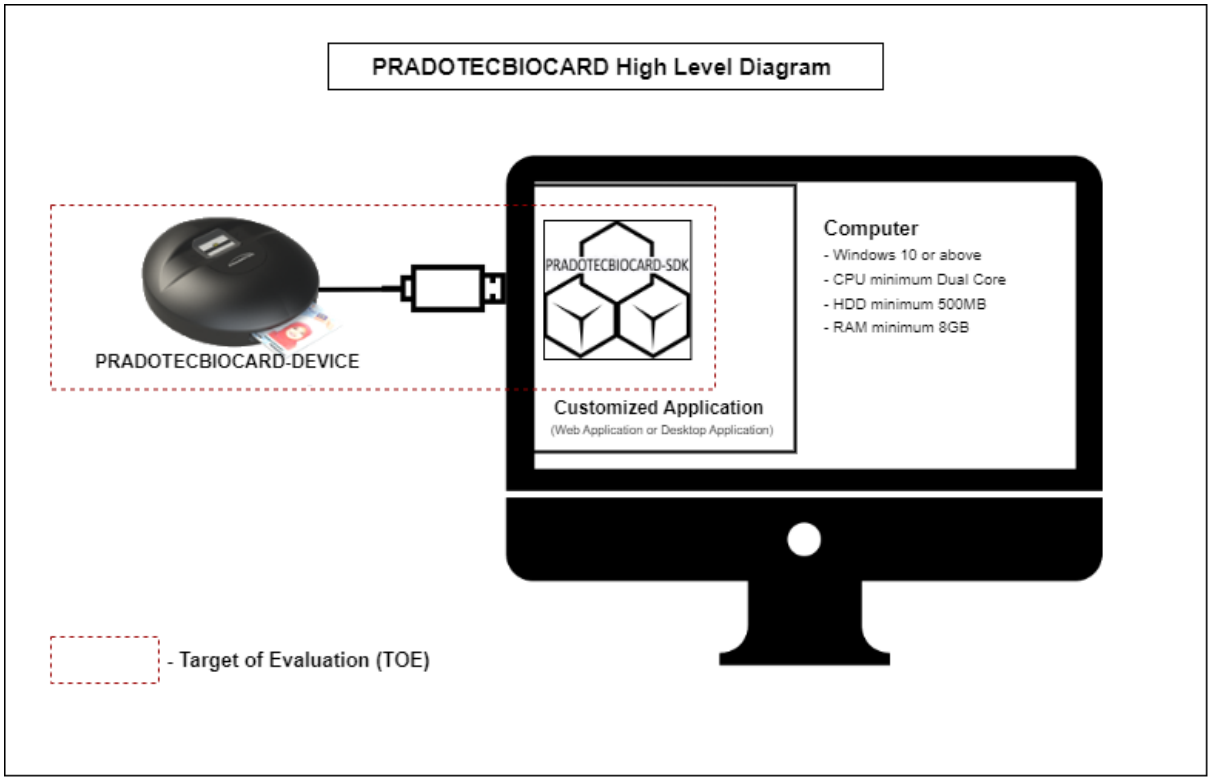

Figure 1 – Pradotec BioCard High Level Diagram

The major security features of the TOE included in the evaluation is:

- Identity Verification
    - 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. (Note: MyKid card does not have stored fingerprint templates and thus it is unable to undergo fingerprint verification)

      The combined use of the identity card and thumbprint ensures a stringent validation, confirming the user's identity before granting further action, thereby fortifying the overall security of the verification process.
- Protection of TSF
    - The Pradotec BioCard 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.

For more details, refer to Logical Scope Section.

1.5.2 TOE Type

Pradotec BioCard is essentially a wired biometric smart card reader designed specifically for reading Malaysian Identity Cards and perform thumbprint verification process. Its primary function revolves around reading and processing data from Malaysian Identity Cards and conducting thumbprint verification via the integrated Thumbprint sensor. Therefore, it can be categorised as a Smart Card Reader product.

1.5.3 Non-TOE hardware/firmware/software required by the TOE

The following figure shows the typical operational environment of the TOE.

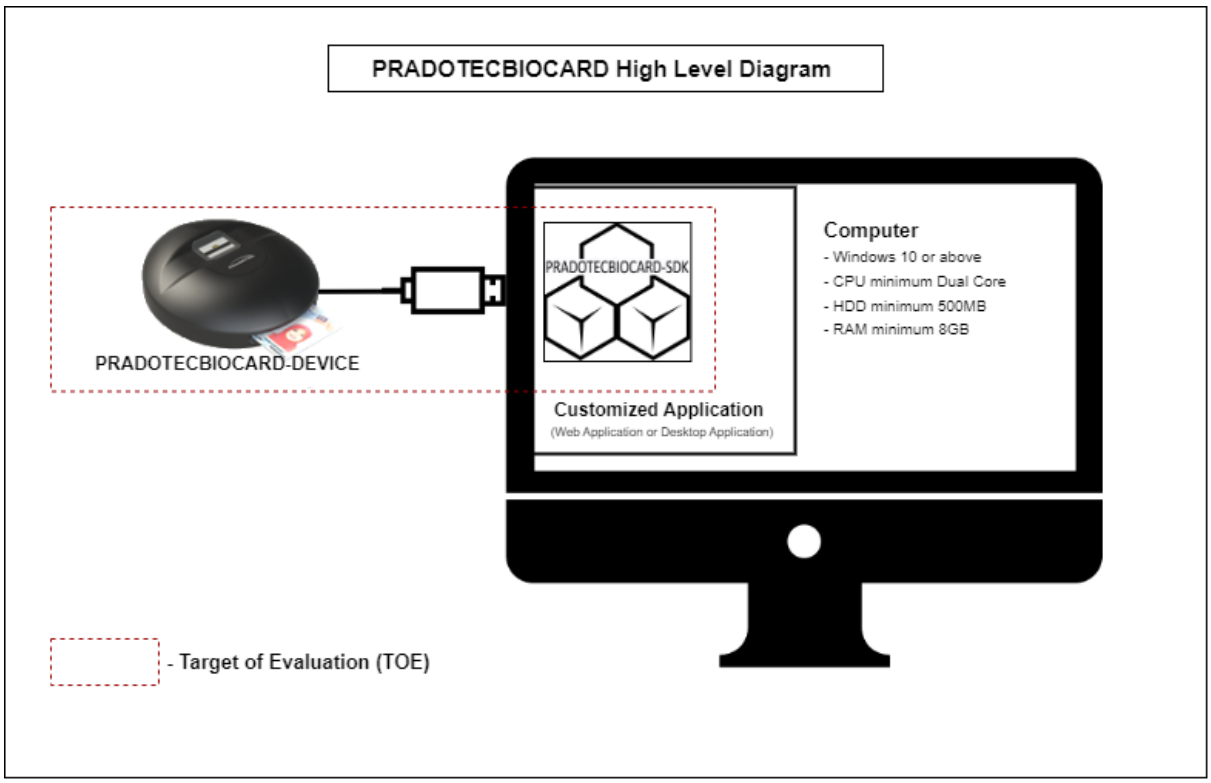

Figure 2 – TOE typical operational environment

Minimum Requirement for PRADOTECBIOCARD-SDK:

- Windows 10 or above
- CPU minimum Dual Core
- HDD minimum 500MB
- RAM minimum 8GB

1.6 TOE Description

Figure 2 – TOE typical operational environment 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.

This section primarily addresses the physical and logical components of the TOE included in the evaluation.

1.6.1 Physical Scope of the TOE

As illustrated in Figure 2 – TOE typical operational environment, the TOE consists of two main components:

- PRADOTECBIOCARD-DEVICE: Pradotec BioCard Hardware Device and
- PRADOTECBIOCARD-SDK: Pradotec BioCard Web-based Software Development Kits

1.6.1.1 Delivery Method

The two components of the TOE will be delivered separately.

The PRADOTECBIOCARD-DEVICE will be sealed in a 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.

1.6.2 Logical Scope of the TOE

The logical scope of TOE is described based on the following security functional requirement.

1.6.2.1 Identity Verification

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.

1.6.2.2 Protection of TSF

The Pradotec BioCard 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.

2 Conformance Claims

The following conformance claims are made for the TOE and ST:

CCv3.1 conformant	The ST and the TOE are Common Criteria conformant to Common Criteria version 3.1 Revision 5.
Part 2 conformant	The ST is Common Criteria Part 2 conformant.
Part 3 conformant	The ST is Common Criteria Part 3 conformant.
Package conformant	EAL 1.
Protection Profile conformance	None.

3 Security Objectives

Security objectives are described as below.

3.1 Security Objectives for the Operational Environment

The security objectives for the TOE operational environment as following:

OE.USER	The users are trusted; the users shall not maliciously compromise the security functionality of the TOE. The users are well trained; the user shall comply with the operating procedures stipulated in the user guidance.
OE.SDK	Establish secure integration guidelines and procedures that verify the authenticity and integrity of the SDK components before integration. This objective aims to ensure that only genuine and validated SDK versions, free from tampering or malicious alterations, are utilized for interaction with the TOE.
OE.PHYSICAL	The TOE and its environment shall be physically secure. Implement measures to secure the physical environment where the TOE is deployed/implemented, including controlled access, surveillance, and protection against theft or unauthorized physical access.

Table 6: Security Objectives for the Operational Environment

4 Extended Components

This section defines the extended Security Functional Requirements (SFRs) and extended Security Assurance Requirements (SARs) applicable for the TOE.

4.1 Extended Security Functional Requirement (SFR)

There are no extended SFR components defined for this evaluation.

4.2 Extended Security Assurance Requirement (SAR)

There are no extended SAR components defined for this evaluation.

5 TOE Security Requirements

This section provides the security functional and assurance requirements that must be satisfied by a compliant TOE. These requirements consist of functional components from Part 2 of the CC, extended requirements, and an Evaluation Assurance Level (EAL) that contains assurance components from Part 3 of the CC.

5.1 Conventions

Part 2 of the Common Criteria defines an approved set of operations that may be applied to the statement of security functional requirements. Following are the operations and the document conventions as used within this ST to depict their application:

Assignment	The assignment operation provides the ability to specify an identified parameter within a requirement. Assignments are depicted using bolded text and are surrounded by square brackets as follows [**assignment**].
Selection	The selection operation allows the specification of one or more items from a list. Selections are depicted using bold italics text and are surrounded by square brackets as follows [***selection***].
Refinement	The refinement operation allows the addition of extra detail to a requirement. Refinements are indicated using bolded text, for **additions**, and strike-through, for ~~deletions~~.
Iteration	The iteration operation allows a component to be used more than once with varying operations. Iterations are depicted by placing an acronym at the end of the component identifier as follows: FCS_COP.1 (SWP).

5.2 Security Functional Requirements (SFR)

This section contains the security functional requirements (SFRs) for the TOE. The summary of SFRs is listed in following table.

Component	Component Name
Class FIA: Identification and authentication	
FIA_UID.2	User identification before any action
Class FPT: Protection of the TSF	
FPT_PHP.1	Passive detection of physical attack

Table 7: Security Functional Requirements List

5.2.1 Class FIA: Identification and Authentication

FIA_UID.2 User identification before any action

Hierarchical	FIA_UID.1 Timing of identification
Dependencies	No dependencies.
FIA_UID.2.1	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

5.2.2 Class FPT: Protection of the TSF

FPT_PHP.1 Passive detection of physical attack

Hierarchical	No other components
Dependencies	No dependencies.
FPT_PHP.1.1	The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.
FPT_PHP.1.2	The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.

5.3 Security Assurance Requirements

This ST claims compliance to the assurance requirements from the CC EAL1 assurance package.

The following table summarized the TOE assurance requirements drawn from CC Part 3.

Assurance Class	Assurance components
ADV: Development	ADV_FSP.1 Basic functional specification
AGD: Guidance Documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Lifecycle Support	ALC_CMC.1 Labelling of the TOE
	ALC_CMS.1 TOE CM coverage
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.1 Security objectives for the operational environment
	ASE_REQ.1 Direct rationale security requirements
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_IND.1 Independent testing - conformance
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey

Table 8: Security Assurance Requirements for EAL1

6 TOE Summary Specifications

TOE addressed the security functional requirements as following:

6.1 Identification

The TOE facilitates robust identity verification by integrating with a Malaysian's Identity card, allowing users to initiate the process by inserting the card into the device. Following this, the citizen engages with the TOE's thumbprint sensor to scan their thumbprint (both left and right). This identity verification process, leveraging both the card's data and the individual's biometric information. The combined use of the identity card and thumbprint ensures a stringent validation, confirming the user's

identity before granting further action, thereby fortifying the overall security of the verification process.

Relevant SFR: FIA_UID.2

6.2 Protection of the TSF

TOE shall provide for features that indicate when a TSF device or TSF element is subject to tampering. However, notification of tampering is not automatic; user must perform manual physical inspection to determine if tampering has occurred.

Relevant SFR: FPT_PHP.1