MINISTRY OF DIGITAL

CyberSecurity MALAYSIA

C132 Certification Report

UNIBOX 2.0 v1.0

File name: ISCB-5-RPT-C132-CR-v1
Version: v1
Date of document: 19 June 2024
Document classification : PUBLIC

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

C132 Certification Report

UNIBOX 2.0 v1.0

19 June 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:	C132 Certification Report
DOCUMENT REFERENCE:	ISCB-5-RPT-C132-CR-V1
ISSUE:	V1
DATE:	19 June 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, in order 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 27 June 2024, and the Security Target (Ref**Error! Reference source not found.**). The certification report, Certificate of product evaluation and security target are posted on the MyCC Scheme Certified Product Register (MyCPR) at https://iscb.cybersecurity.my and the Common Criteria Portal (the official website of the Common Criteria Recognition Arrangement).

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	07 June 2024	All	Initial draft
d2	12 June 2024	Pg 22	Updated Evaluation Technical Report Version
v1	19 June 2024	All	Final Version

Executive Summary

The TOE is UNIBOX 2.0 v1.0, which is a secure payment platform which utilizes application programming interface (API) that enables Authorised Users (i.e., merchants) to perform e-commerce transaction with payment channels of choice, inquire and be notified of changes to transaction statuses.

The TOE provide a seamless experience for online merchants to connect to their payment provider of choice. Without utilising the TOE, the online merchants are required to establish an entity in the country that they provide their service and integrate to their payment provider manually.

The TOE provides security functions such as identification and authentication, security management, security audit, trusted path/channels and cryptographic support.

The scope of the evaluation is defined by the Security Target ([6]) which identifies the intended environment for the TOE, 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 Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme (Ref [4]).

The evaluation was performed by Digiforen (M) Sdn Bhd and the evaluation was completed on 23 May 2024.

The Malaysian 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) at https://iscb.cybersecurity.my 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 UNIBOX 2.0 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 TOE is UNIBOX 2.0 v1.0 which owned and developed by the Agiletech Systems (M) Sdn Bhd since January 2022. The TOE is a secure payment platform which was developed to provide an authorised and secure payment channel for merchants to connect with payment providers. The services provided by the TOE include transaction initiation, initiate refunds, payment status inquiries, etc.

2 The TOE also includes an API Management platform which provides front end applications (also known as applet) to perform security management and modify the behaviour of the API.

3 The brand name of the TOE is "UniPin", while the TOE name is "UNIBOX 2.0". The name "UniPin" is understood by the market as the solution provider, hence it's portrayed on the TOE. The key features of the TOE are listed as below:

- Provide the list of payment channels that support the Authorised Users' currency of choice;
- Secure transaction between Authorised Users and payment channels through cryptography;
- Automatic update response from payment provider to the TOE, and from the TOE to Authorised User. This automatic response is called "callbacks", it's one of the transactions.
- Status inquiries for pending transactions or refunds;
- Audit logging of transaction initiations and statuses, and access to the merchant dashboard (i.e., Merchant Access) and API manager (i.e., Merchant Admin);
- Timely notifications if there are updates to the transactions or refunds; and
- Central management applets which allow Super Administrator to manage and modify security behaviour of the TOE, read audit events such as CRUD actions performed by Super Administrator on the TOE and transactions initiated by the Authorised User to the TOE using the API.

- The list below refer for the specific security behaviours of the TOE and Authorised User's security behaviours that can be modified by the Super Administrator:
    - Security behaviour of the TOE modifiable by the Super Administrator:
        i. Password quality metrics;
        ii. Payment channel maintenance; and
        iii. Security of the connection required by the Trusted Path
    - Security behaviour of the Authorised User modifiable by the Super Administrator:
        i. Role and permission;
        ii. Merchant listing;
        iii. Contracts;
        iv. Transaction credentials;
        v. Rate card; and
        vi. Read access to audit logs.

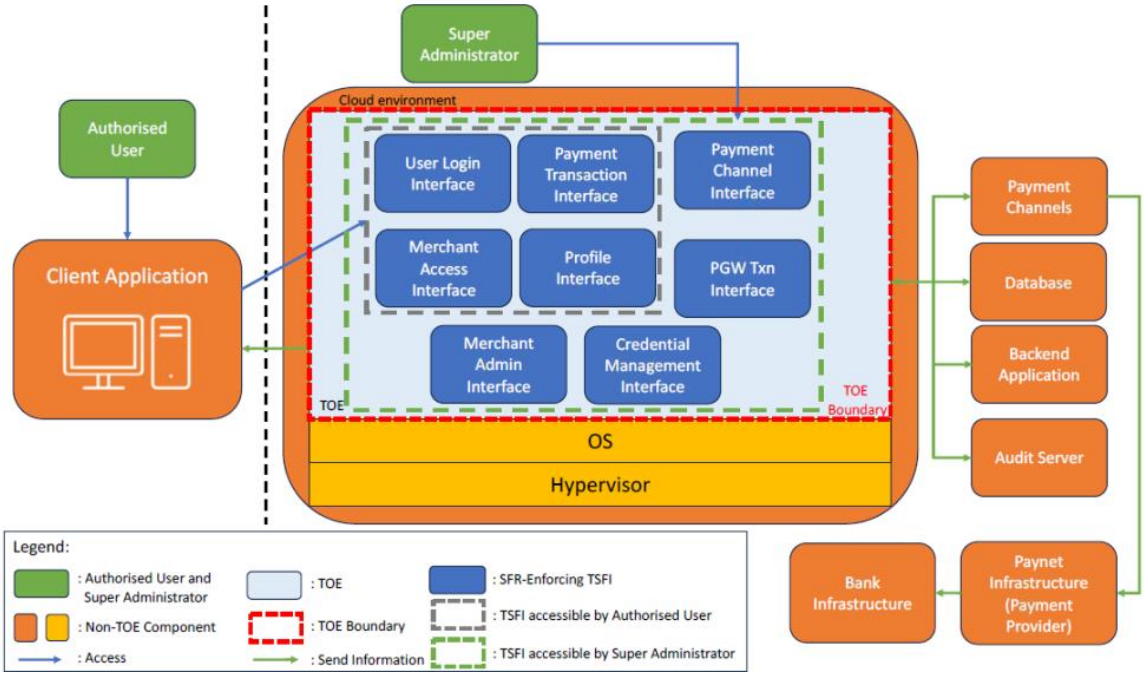

Figure 1: TOE Boundary

4 Figure 1 shows the the TOE boundary and the implementation diagram of how the TOE is accessed. There are two (2) user roles for the TOE which are Authorised User and Super Administrator. The Authorised User are the end-user customers that utilise the TOE. The Authorised User can insert their email or mobile number and password at the User Login Interface to gain access into the TOE. The Super Administrator have the highest privilege on the TOE and are able to authorise Authorised User for specific access.

1.2 TOE Identification

5 The details of the TOE are identified in table below.

Evaluation Scheme	Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme
Project Identifier	C132
TOE Name	UNIBOX 2.0
TOE Version	v1.0
Security Target Title	Agiletech Systems (M) UNIBOX 2.0 v1.0 Security Target
Security Target Version	v1.14
Security Target Date	14 May 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	Agiletech Systems (M) Sdn. Bhd. A-04-03, Tamarind Square Persiaran Multimedia Cyber 10 63000 Cyberjaya Selangor Malaysia.

Developer	Agiletech Systems (M) Sdn. Bhd. A-04-03, Tamarind Square Persiaran Multimedia Cyber 10 63000 Cyberjaya Selangor Malaysia.
Evaluation Facility	Digiforen (M) Sdn Bhd 1-4B, Incubator 3, Technology Park Malaysia, Lebuhraya Puchong-Sungai Besi, Bukit Jalil, 57000 Kuala Lumpur, Wilayah Persekutuan, Malaysia.

Table 1: TOE Identification

1.3 Security Policy

6 No Organisational Security Policy (OSP) declared for the TOE.

1.4 TOE Architecture

7 The TOE consist of logical and physical boundaries which are described in Section 1.7 of the Security Target ([6]).

1.4.1 Logical Boundaries

8 The logical boundary of the TOE is summarized below:

- **Identification and authentication**
  The Authorised Users and Super Administrator are required to insert email or mobile number and password to be authorised and gain access to the central management platform. The quality of password is also controlled, and they're required to be a minimum 8 and maximum 64 characters which includes at least 1 uppercase and 1 lowercase alphabet, 1 numerical character and 1 special character.

  Without properly authenticating and identifying the user's identity, they will not be given access to the TOE.

- **Security management**

  The roles exist for this TOE are Authorised User and Super Administrator. All users are required to insert email address or mobile number and password before they are able to use any TOE security functions.

  The Authorised User is defined as the TOE consumer. The TOE restricts the access of Authorised Users only to the management functions which are determined by the Super Administrator. The Authorised Users are able to modify their own mobile number and password.

  Super Administrator are the TOE's developers that have the highest privilege of the TOE and are able to modify the security behaviour of the TOE and Authorised Users, such as:

  - Security behaviour of the TOE modifiable by the Super Administrator:
    i. Modify login contact number and password
    ii. Password quality metrics;
    iii. Payment channel maintenance; and
    iv. Security of the connection required by the Trusted Path
  - Security behaviour of the Authorised User modifiable by the Super Administrator:
    i. Role and permission;
    ii. Merchant listing;
    iii. Contracts;
    iv. Transaction credentials;
    v. Rate cards; and
    vi. Read access to audit logs.

- **Security audit**

  Audit entries are generated for security related events on some of the TOE components (i.e., Authorised User's transactions through API, Super Administrator's modifications made to applets on the TOE, etc.). The audit logs are only accessible (i.e., read access) by the Super Administrator. The audit logs are stored on an external audit server where the communication is secured through TLS v1.2 and above.

  The audit logs are not allowed to be modified and deleted.

- **Trusted path/channels**
  The TOE is able to protect the user data from unauthorised modifications and disclosures by securing the communication channel with cryptography. The channels are secured between the user and the TOE such as:
  1) Initial user authentication
  2) Transaction initiations from Authorised User to the TOE through API;
  3) Transaction callbacks from the TOE to the Authorised User; and
  4) Access to the TOE by Super Administrator and Authorised User.
- **Cryptographic support**
  The TOE is able to perform SHA-256 hashing cryptographic operations to ensure the authenticity of the transactions, through utilisation of the Merchant_code and Merchant_key within the pre-determined formulae.

  These Merchant_code and Merchant_key are generated by the Super Administrator, and they will inform the specific Authorised User of their Merchant_code and Merchant_key through email.

  The Merchant_code and Merchant_key are the main variables in differentiating between an authentic transaction and a forged transaction. The pre-determined formulae will ensure that only the original Authorised User can achieve the same hash as the Super Administrator.

1.4.2 Physical Boundaries

9 The TOE comprise of the following:

- The TOE software, i.e. UNIBOX 2.0 v1.0

10 The non-TOE comprise of the following:

- **Transport Layer Security.**
  Cryptography of the communication channel between users to the TOE; and from TOE to other trusted IT products such as database, backend application, payment channels and audit servers with TLS v1.2 and above is provided by CloudFlare.
- **Secret Connection to Other Trusted IT Product**.

  The connections between the TOE and other trusted IT product such as databases, backend applications, payment channels, and audit servers are secured through Virtual Private Cloud (VPC) provided by AWS Cloud.
- **Database Server**

The TOE will complete the request by parsing it to external PostgreSQL database servers located in cloud.

- **Backend Applications**

  Auxiliary applications to support the implementation of the API.

- **Payment Channels**

  The TOE will complete the request by parsing it to external payment channels' web servers. This is not to be confused with the Payment Channel applet.

- **Time Server**

  The TOE utilizes Network Time Protocol (NTP) server to synchronize its system clock with a central time source.

- **Client Applications**

  The TOE accepts request through HTTP protocol, hence the TOE can be called through browser address bar or Command Line Interface that support cURL command such as PowerShell.

- **Platform for the TOE**

  This TOE component operates on Tomcat Apache, with the following operating systems (OS) in cloud:

  a) Alpine Linux version 3 and later (For API)
  b) CloudFlare pages (For Applets)

- **Access for the TOE**

  This TOE component can be accessed through the following web browsers:

  a) Internet Explorer 8, 9, 10, 11; and
  b) Chrome 55 or higher.

  NOTE: The evaluation of the TOE components are performed on Chrome 118

- **Audit Server**

  Used for external storage of audit data.

1.5 Clarification of Scope

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

12 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]).

13 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

14 This section is not applicable for EAL1.

1.7 Evaluated Configuration

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

16 As stated in Security Target (Ref[6]), the TOE is a secure payment platform which utilizes application programming interface (API) that enables Authorised Users (i.e., merchants) to perform e-commerce transaction with payment channels of choice, inquire and be notified of changes to transaction statuses.

17 The TOE is accessed via the URL: https://bo.unipin.dev/ using Chrome version 118 on Windows 10 Pro version 22H2 with screen lock mechanism enabled.

18 The TOE is accessed on devices that are accessible only to authorised personnel.

19 The TOE is accessed and operated by the evaluators and uses the software within compliance of the guidance.

20 The TOE is delivered as a web application by the developer in its known state.

1.8 Delivery Procedures

21 This section in not applicable for EAL1.

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 checked that the TOE references use are consistent.

26 The evaluator examined the configuration list to determine that it uniquely identifies each configuration item.

27 At the end, the evaluator confirmed that all the requirements for this class were fulfilled and passed.

2.1.2 Development

28 The evaluator examined the functional specification described the purpose and method of use for each SFR-enforcing TSFI.

29 The evaluator examined the presentation of the TSFI to determine that it identifies all parameters associated with each SFR-enforcing TSFI.

30 The evaluator traced that the SFRs trace to TSFIs in the functional specification.

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

32 At the end, the evaluator confirmed that all the requirements for this class were fulfilled and passed.

2.1.3 Guidance documents

33 The evaluator examined the TOE preparative user guidance and operational user guidance, and determined that it sufficiently and unambiguously described how to securely transform the TOE into its evaluated configuration, and how to use and administer the product in order to fulfil the security objectives for the operational environment.

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

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

2.1.4 IT Product Testing

36 Testing at EAL 1 consists of performing independent functional test and conducting penetration tests. The TOE testing was conducted by Digiforen (M) Sdn Bhd. The detailed testing activities including configurations, procedures, test cases, expected results and actual results are documented in a separate Test Plan Report (TPR).

2.1.4.1 Independent Functional Testing

37 At EAL 1, provides an evaluation of the TOE as made available to the customer, including independent testing against a specification, and an examination of the guidance documentation provided. It is intended that an EAL1 evaluation could be successfully conducted without assistance from the developer of the TOE, and for minimal outlay.

38 All an evaluation at this level should provide evidence that the TOE functions in a manner consistent with its documentation.

Test Title	Test Title	Description	Security Function	TSFI	Results
TEST GROUP A – Identification and Authentication					
1.	A1. Login as Super Administrator	To test whether Super Administrator and Authorised User able to perform identification and authentication functions to the TOE.	FIA_UID.2 FIA_ATD.1 FIA_UAU.2 FAU_GEN.1 FIA_SOS.1	User Login Interface	Passed
2.	A2. Login as Authorised User				Passed
TEST GROUP B- Security Management					
3.	B1(a). Super Administrator - Assign and remove role access for Authorised User	To test whether the Super Administrator able to perform management functions: • Assign and remove role access for Authorised User	FMT_SMF.1(1) FMT_SMR.1 FMT_MTD.1(1) FAU_GEN.1 FAU_SAR.1	Merchant Admin Interface	Passed
4.	B1(b). Super Administrator - Assign and remove permission for Authorised User	To test whether the Super Administrator able to perform management functions: • Assign and remove permission for Authorised User.			Passed
5.	B1(c). Super Administrator - Assign and remove the Authorised User's merchant	To test whether the Super Administrator able to perform management functions: • Assign and remove the			Passed

Test Title	Test Title	Description	Security Function	TSFI	Results
	listing and contracts	Authorised User's merchant listing and contracts.			
6.	B1(d). Super Administrator - Assign and activate the rate cards for the contracts of the Authorised User	To test whether the Super Administrator able to perform management functions: • Assign and activate the rate cards for the contracts of the Authorised User.			Passed
7.	B1(e). Super Administrator - Assign an initial email or mobile number and password for Authorised User	To test whether the Super Administrator able to perform management functions: • Assign an initial email or mobile number and password for Authorised User.	FIA_UID.2 FIA_ATD.1 FIA_UAU.2 FIA_SOS.1 FMT_SMF.1(1) FMT_MTD.1(1) FAU_GEN.1	Credential Management Interface	Passed
8.	B1(f). Super Administrator - Assign and activate the contracts, rates, and connections to payment channels	To test whether the Super Administrator able to perform management functions: • Assign and activate the contracts, rates, and connections to payment channels.	FMT_SMF.1(1) FMT_MTD.1(1) FAU_GEN.1	Payment Channel Interface	Passed
9.	B1(g). Super Administrator - Modification of Super Administrator's	To test whether the Super Administrator able to perform management functions:	FMT_SMF.1(1) FMT_SMR.1 FMT_MTD.1(1) FIA_SOS.1 FIA_UID.2 FIA_ATD.1	Profile Interface	Passed

Test Title	Test Title	Description	Security Function	TSFI	Results
	login contact number and password	• Modification of Super Administrator's login contact number and password	FIA_UAU.2		
10.	B1(h) Super Administrator - To restrict the read access to audit logs only to Super Administrator.	To test whether the Super Administrator able to perform management functions: • To restrict the read access to audit logs only to Super Administrator.	FMT_SMF.1(1) FMT_SMR.1 FMT_MTD.1(1) FIA_SOS.1 FAU_GEN.1 FAU_SAR.1	Merchant Admin Interface Payment Channel Interface	Passed
11.	B2(a). Authorised User-Modification of Authorised User's mobile number and password	To test whether the Authorised User able to perform management functions: • Modification of Authorised User's mobile number and password.	FMT_SMF.1(2) FMT_SMR.1 FMT_MTD.1(2) FIA_SOS.1	Profile Interface	Passed
12.	B2(b). Authorised User-Accept the Offered Contracts	To test whether the Authorised User able to perform management functions: • Accept the offered contracts.	FMT_SMF.1(2) FMT_MTD.1(2)	Merchant Access Interface	Passed
13.	B2(c). Authorised User-Read access to the following operations, i. current transactions	To test whether the Authorised User able to perform management functions:			Passed

Test Title	Test Title	Description	Security Function	TSFI	Results
	ii. successful transactions iii. pending transactions iv. failed transactions iv. refunds v. cancelled transactions	• Read access to the following operations, i. current transactions ii. successful transactions iii. pending transactions iv. failed transactions v. refunds vi. cancelled transaction			
TEST GROUP C- Security Audit					
14.	C1. Transaction Initiation	To generate the audit record after performing the transactions. • All transaction initiated by the Authorised User to the TOE through API, such as transaction initiation;	FAU_GEN.1 FAU_GEN.2	Payment Transaction Interface	Passed
15.	C2. Transaction Callback	To generate the audit record after performing the transactions. • All transaction initiated by the Authorised User to the TOE through API, such as initiate refund;			Passed
16.	C3. Initiate Refund	To generate the audit record after performing the transactions.			Passed

Test Title	Test Title	Description	Security Function	TSFI	Results
		• All transaction initiated by the TOE to the Authorised User through API, such as transaction callback;			
17.	C4. Refund Callback	To generate the audit record after performing the transactions. • All transaction initiated by the TOE to the Authorised User through API, such as refund callback.			Passed
TEST GROUP D – Cryptographic Support					
18.	D1. Get Payment Channel List (Signature)	To test for hashing cryptography on Get Payment Channel List (Signature)	FCS_COP.1	Payment Transaction Interface	Passed
19.	D2. Transaction Initiation (Signature)	To test for hashing cryptography on Transaction Initiation (Signature)			Passed
20.	D3. Transaction Callback (Signature)	To test for hashing cryptography on Transaction Callback (Signature)			Passed
21.	D4. Transaction Inquiry (Signature)	To test for hashing cryptography on			Passed

Test Title	Test Title	Description	Security Function	TSFI	Results
		Transaction Inquiry (Signature)			
22.	D5. Initiate Refund (Signature)	To test for hashing cryptography on Initiate Refund (Signature)			Passed
23.	D6. Callback (Signature)	To test for hashing cryptography on Refund Callback (Signature)			Passed
24.	D7. Get Transaction Merchant Report (Signature)	To test for hashing cryptography on Get Transaction Merchant Report (Signature)			Passed
25.	D8. Get Merchant Balance (Signature)	To test for hashing cryptography on Get Merchant Balance (Signature)			Passed
TEST GROUP E- Trusted Path/Channels					
26.	E1. Check TLS Version for Initial User Authentication	To test whether the communication channel between the Super Administrator and Authorized User involves the use of TLS v1.2 and above for initial user authentication.	FTP_TRP.1	User Login Interface	Passed
27.	E2. Check TLS Version for Transaction Initiations from Authorised User	To test whether the communication channel between the Super Administrator and			Passed

Test Title	Test Title	Description	Security Function	TSFI	Results
	to TOE through API and Transaction Callbacks from TOE to Authorised User	Authorized User involves the use of TLS v1.2 and above for transaction initiations from the Authorised User to the TOE through API and transaction callbacks from the TOE to the Authorised User		Payment Transaction Interface	
TEST GROUP F- Security Audit					
28.	F1. Super Administrator - Read Access to Audit Logs for Transaction Initiation	To test whether the Super Administrator has the permission to read access to Audit logs in Transaction which is all transaction initiated by the Authorised User to the TOE through API such as Transaction Initiation.	FAU_SAR.1	PGW Txn Interface	Passed
29.	F2. Super Administrator - Read Access to Audit Logs for Initiate Refund	To test whether the Super Administrator has the permission to read access to Audit logs in Transaction which is all transaction initiated by the Authorised User to the TOE through API such as Initiate Refund.	FAU_SAR.1	PGW Txn Interface	Passed
30.	F3.	To test whether the Super	FAU_SAR.1		Passed

Test Title	Test Title	Description	Security Function	TSFI	Results
	Super Administrator - Read Access to Audit Logs for Transaction Callback	Administrator has the permission to read access to Audit logs in Transaction which is all transaction initiated by the TOE to the Authorised User through API such as Transaction Callback.		PGW Txn Interface	
31.	F4. Super Administrator - Read Access to Audit Logs for Refund Callback	To test whether the Super Administrator has the permission to read access to Audit logs in Transaction which is all transaction initiated by the TOE to the Authorised User through API such as Refund Callback.			Passed
32.	F5. Super Administrator - Read the security audit log for CRUD actions performed by Super Administrator on the TOE	To test whether the Super Administrator has the permission to read access to read the security audit log for CRUD actions performed by Super Administrator on the TOE such as: a. Create merchant; b. Edit merchant; c. Delete merchant;	FAU_SAR.1 FMT_SMF.1(1)	Merchant Admin Interface Payment Channel Interface	Passed

Test Title	Test Title	Description	Security Function	TSFI	Results
		d. Create contract; e. Edit contract; f. Remove contract; g. Create rate card; h. Remove rate card; i. Create charge rate; j. Edit charge rate; k. Remove charge rate; l. Adding rate; m. Editing rate; n. Deleting percentage rate; and o. Deleting fixed rate.			

Table 2: Functional Test

39 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 evaluators and are consistent with the expected test results in the test documentation.

40 All testing performed by evaluators produced the expected results and as such the TOE behaved as expected.

2.1.4.2 Vulnerability Analysis

41 The evaluators 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, functional specification, TOE design, and security architecture description.

42 From the vulnerability analysis, the evaluators 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

43 The penetration tests focused on:

a) SQL Injection (SQLi)

b) Cross-site Scripting (XSS)

c) File Upload

d) Iframe Injection

e) Insecure Direct Object Reference (IDOR)

f) Directory Listing

g) Local File Inclusion

h) Sniffing

i) Intercept

44 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

45 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

46 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 UNIBOX 2.0 v1.0 which is performed by Digiforen (M) Sdn Bhd.

47 Digiforen (M) Sdn Bhd found that UNIBOX 2.0 v1.0 upholds the claims made in the Security Target (Ref **Error! Reference source not found.**) and supporting documentations, and has met the requirements of the Common Criteria (CC) Evaluation Assurance Level 1.

48 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

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

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

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

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

3.2 Recommendation

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

a) Opinions and interpretations expressed herein are outside the scope of accreditation.

b) It is recommended that all guidance outlined in Preparative Guidance and Operational Guidance be followed to configure the TOE in the evaluated configuration.

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, July 2023.

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

[6] Agiletech Systems (M) UNIBOX 2.0 v1.0 Security Target, v1.14, 14th May 2024.

[7] Digiforen (M) Sdn Bhd MP-230804-92 Evaluation Technical Report UNIBOX 2.0 v1.0, v1.1, 12th June 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 ---