MINISTRY OF COMMUNICATIONS
AND MULTIMEDIA MALAYSIA

CyberSecurity MALAYSIA

C119 Certification Report

SecurePay Platform v4.9.1

File name: ISCB-5-RPT-C119-CR-v1
Version: v1
Date of document: 10 June 2021
Document classification: PUBLIC

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

CyberSecurity Malaysia
(726630-U)
Corporate Office:
Level 7, Tower 1
Menara Cyber Axis
Jalan Impact
63000 Cyberjaya
Selangor Darul Ehsan
Malaysia.
T +603 8800 7999
F +603 8008 7000
H 1 300 88 2999
www.cybersecurity.my

C119 Certification Report

SecurePay Platform v4.9.1

10 June 2021

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:	C119 Certification Report
DOCUMENT REFERENCE:	ISCB-5-RPT-C119-CR-v1
ISSUE:	v1
DATE:	10 June 2021
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 16 June 2021, 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 www.cybersecurity.my/mycc 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	4 June 2021	All	Initial draft
V1	10 June 2021	All	Final Release

Executive Summary

The Target of Evaluation (TOE) is SecurePay Platform v4.9.1. The TOE is a secure payment processing platform that enable users to perform e-commerce transaction, sending bills, bulk payments, collections and statutory payments. The TOE provides security functionality such as Secure Payment, Security Audit, Identification and Authentication and Security Management.

The scope of the evaluation is defined by the Security Target (Ref[6]) which identifies assumptions made during the evaluation, 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 2 (EAL2). 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 Securelytics SEF and the evaluation was completed on 19 May 2021.

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) at http://www.cybersecurity.my/mycc 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 SecurePay Platform v4.9.1 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 SecurePay Platform v4.9.1. The TOE is a software platform as a service whilst installed, configured and deployed on an enterprise cloud environment. The TOE is used by corporate, SME's or merchants as a secure payment processing platform for their customers. Users also able to perform e-commerce transaction, sending bills, bulk payments, collections and statutory payments. The TOE is connected to various banks which facilitate same day processing, ensure data integrity, reduces processing discrepancies and faster response time. It is simple, robust, user friendly, scalable, secured and available 24x7.

2 Below are the primary features of the TOE:

a) E-Commerce - Users able to use the TOE as an e-commerce portal and conduct business over the internet

b) Collection - Users able to create bill form and payment form for their customers

c) Payment Processing - The TOE provides a secure payment processing platform and it is connected to various major banks in Malaysia

d) API integration - Third-party developers able to use and access the TOE via API integrations

3 The following table highlights the range of security functions implemented by the TOE:

Table 1: Security Function

Security Function	Description
Secure Payment	The TOE able to protect the user data and payment transaction from disclosure and modification by using HTTPS (TLS v1.2). Domain securepay.my is signed with DNSSEC. DNSSEC creates a secure domain name system by adding cryptographic signatures to existing DNS records.
Identification & Authentication	The TOE requires that each user is successfully identified and authenticated before any interaction with protected resources is permitted.

Security Function	Description
Security Management	The TOE provides functions that allow management of the TOE and its security functions. The TOE restricts access to the management functions based on the role of the user.
Security Audit	The TOE generates audit records for security events. Admin and Authorised User has the ability to view and export the audit and transaction logs.

1.2 TOE Identification

4 The details of the TOE are identified in Table 2: TOE Identification below.

Table 2: TOE Identification

Evaluation Scheme	Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme
Project Identifier	C119
TOE Name	SecurePay Platform
TOE Version	V4.9.1
Security Target Title	SecurePay Security Target
Security Target Version	V1.0
Security Target Date	23 April 2021
Assurance Level	Evaluation Assurance Level 2
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 2
Sponsor	SecurePay Sdn Bhd A-3A-13, Blok A, Radia Office, Persiaran Arked, Bukit Jelutong, 40150 Shah Alam, Selangor

Developer	SecurePay Sdn Bhd A-3A-13, Blok A, Radia Office, Persiaran Arked, Bukit Jelutong, 40150 Shah Alam, Selangor
Evaluation Facility	Securelytics SEF A-19-06, Tower A, Atria SOFO Suites, Petaling Jaya, Selangor Darul Ehsan

1.3 Security Policy

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

1.4 TOE Architecture

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

1.4.1 Logical Boundaries

7 The logical boundary of the TOE is summarized below:

- Secure Payment

  The TOE can protect the user data and payment transaction from disclosure and modification by using HTTPS (TLS v1.2). Domain securepay.my is signed with DNSSEC. DNSSEC creates a secure domain name system by adding cryptographic signatures to existing DNS records.

- Identification & Authentication

  All users are required to be identified and authenticated before any information flows are permitted. At the login page, TOE users need to key in a valid email and password in order to access the TOE. The acceptable minimum password length is 8-characters. The TOE checks the credentials presented by the user against the authentication information stored in the database.

- Security Management

  The TOE contains various management functions to ensure efficient and secure management of the TOE. The TOE restricts access to the management functions based on the role of the user. The TOE defines two security management roles: Admin and Authorised User. Refer below:

a) Admin user has the ability to perform Announcements management, Users management, Accounts management, Banks management, Payments management, External Payments management, Plans management, Domains management, Admins management, Feedbacks management, View & Export Audits and Options management.

b) Authorised user has the ability to perform Collections management, Catalogs management, Stores management, Products management, Shippings management, Discounts management, Customers management, Accounts management and API management.

- Security Audit
  The TOE generates audit records for security events. The Admin and authorised user have the ability to view and export the audit logs. The types of audit logs are:
  a) Payment Transaction Status
  b) Bill Transaction Status
  c) Settlements Transaction Status
  d) User Signed In/ Signed Out
  e) Changes on user account

1.4.2 Physical Boundaries

8 A typical implementation of the TOE can be found in Figure 1 below, which identifies the various components of the TOE architecture.

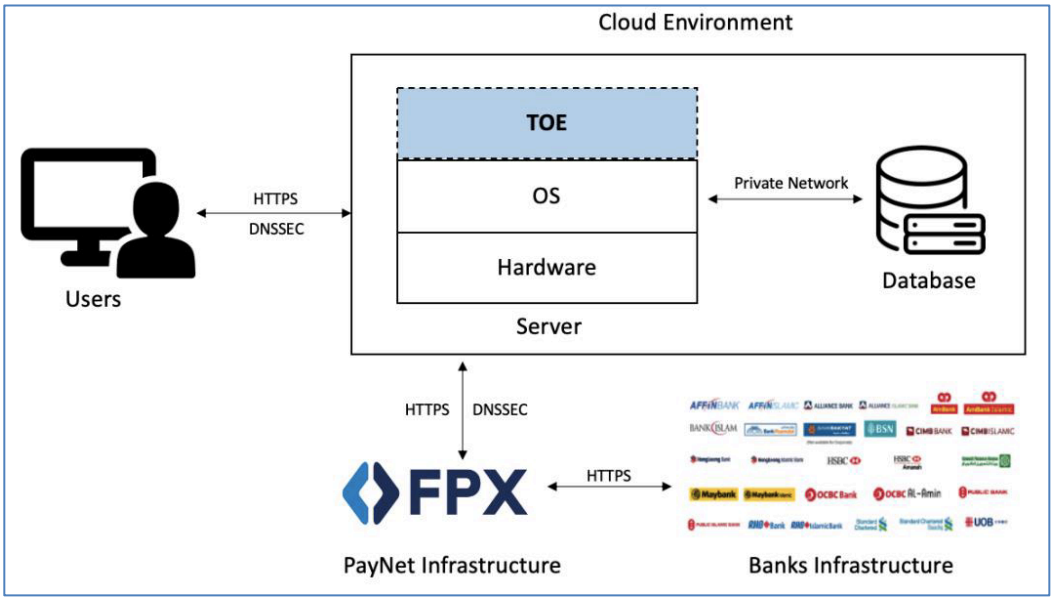

Figure 1 – TOE

9 The users are accessing the TOE via the internet connection. The primary access to the TOE is via a web application by browsing to https://www.securepay.my or via API (API URL for merchant integration is https://securepay.my/api). Merchant can access the information via API and received the json format response.

1.5 Clarification of Scope

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

11 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]).

12 Potential consumers of the TOE are advised that some functions and services of the overall product have not have 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

13 This section summarises the security aspects of the environment/configuration in which the product is intended to operate. Consumers should understand the requirements for secure operation of the TOE as defined in the Security Target (Ref [6]).

1.6.1 Environmental assumptions

14 Assumptions for the TOE environment as described in the Security Target (Ref [6]):

Table 3: Assumptions for the TOE Environment

Environment	Statement
A.NOEVIL	It is assumed that the person who manages the TOE is not hostile and is competent.
A.NOTRST	The TOE can only be accessed by authorized users.
A.CLOUD	The cloud environment will provide a load balancing, web application firewall (WAF) and network traffic filters (e.g. access control lists (ACL)) services in order to prevent the attacker from performing any malicious activity against the TOE and to prevent application failure.

A.TIMESTAMP	The underlying operating system will have a reliable time source that the TOE can utilize for generating audit log timestamps.

1.7 Evaluated Configuration

15 This section describes the configurations of the TOE that are included within the scope of the evaluation. The evaluated configuration for TOE is the software platform as a service that has been installed, configured and deployed on an enterprise cloud environment in accordance with the Guidance documents and Security Target.

16 As depicted in Figure 2 below, the TOE has the following TSFI:

- **ADMIN Interface (SFR-enforcing).** The ADMIN interface provides user interface for Admin to interface with the TOE and perform Admin functions.
- **USER Interface (SFR-enforcing).** The USER interface provides user interface for Authorised Users to login and perform Authorised user functions
- **SEC_API (SFR-enforcing).** The programming interface used to engage the TLS and DNSSEC functionality of the TOE and provide secure communication channel between the TOE and user's web browser to protect user data and payment transaction.

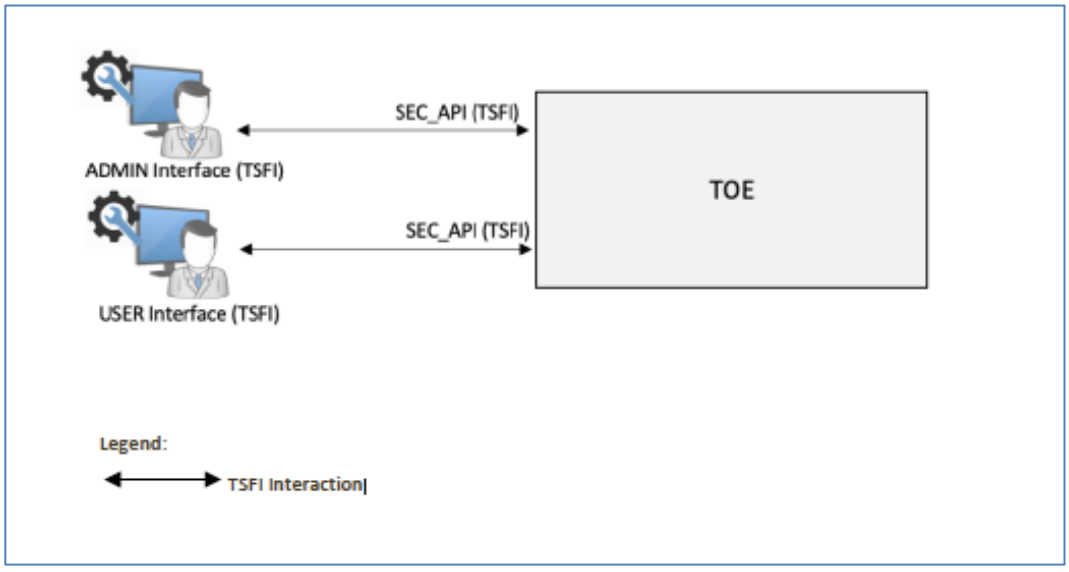

Figure 2 - Evaluated Deployment Configuration of the TOE

17 Figure 3 below provides a detailed architectural view of the various subsystems that comprise the TOE.

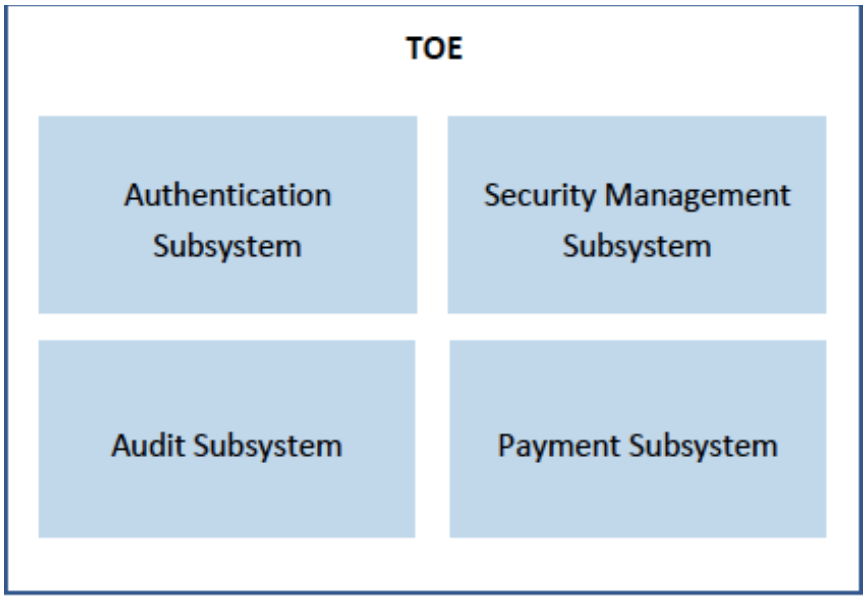

Figure 3 - Detailed architectural view of the TOE

18 Each of the subsystems identified within the TOE is summarised and categorised in the following table:

Table 4 - Summary of Subsystems

Subsystem	Overview	Category
Payment Subsystem	Provides transport layer protection between the TOE and user's web browser by implementing Transport Layer Security (TLS v1.2) protocol.	SFR-enforcing
Audit Subsystem	Implements the capability to generate audit record and only accessible from the web interface	SFR-enforcing
Authentication Subsystem	Implements both the identification and authentication capabilities for the TOE	SFR-enforcing
Security Management Subsystem	Implements the capability to perform operations in Section 6.4 in ST.	SFR-enforcing

1.8 Delivery Procedures

19 The evaluators examined the delivery documentation and determined that it describes all procedures that are necessary to maintain security when distributing versions of the TOE or parts of it to the consumer.

20 The evaluators also examined the aspects of the delivery process and determined that the delivery procedures are used.

1.8.1 TOE Delivery Procedures

21 The delivery of the TOE from the development and build environment to the production server goes through the following phases:

a) **Information Gathering**: SecurePay will gather requirements from the following 2 sources; Customers' feedback / request and research by SecurePay internal product business owners. Once the requirements are listed, product business owners, designers and developers will have an internal meeting and the designers will finalize the functional designs.

b) **Development and build:** The development and build process are controlled within SecurePay's development environment. Designers and developers will collaborate to build or enhance products to meet the requirements.

c) **Released:** A specific set of procedures are followed before a new version of the TOE or any key component can be released, these procedures include the following:

i. A pre-release meeting will be held to determine all relevant documents are in place.

ii. The pre-release meeting will also determine the release version of the Applications.

iii. The release date will be established.

iv. Codes are migrated to the build server, which resides in the cloud infrastructure through secured connections (SSL).

v. Test build of the application is deployed to the protected environment and go through QA process.

vi. Production build of the application is compiled and packaged in the build server. The application is compiled and packaged in the build server.

vii. The release version will be then reflected correctly into the corresponding documents, ie, Modules/Bug Fix tracking, Process Flow Diagram and Data Flow Diagram.

viii. All documents to be submitted for approval by respective Managers.

ix. Notification will be sent out to respective Clients to notify the blackout period prior to Release.

d) **Delivery and acceptance:** Once the new version of the TOE or key application component is released it is verified by the developers by checking the version of the TOE and checking the version with the Release logs. Only after a successful verification will the TOE be accepted and be put onto production server for use. In order for the TOE users to access the TOE, TOE users need to browse to https://www.securepay.my and register for an account. At the main page of the website, TOE users can click on the 'Sign In' button and fill in all the necessary information. The password must be at least 8 characters. After the registration process, TOE users will receive an email and able to start using the TOE.

e) **Product technical support:** TOE users will contact SecurePay's Customer Success (CS) team via https://www.securepay.my/contact/ when they have any issues in operating the TOE. However, if the issue involves technical issues (such as data issue) that can't be resolve via email, then the CS team will hand over the issue to a corresponding product's developers for further investigation.

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 2. 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 An analysis of the TOE configuration management system and associated documentation was performed. The evaluators found that the configuration items were clearly and uniquely labelled, and that the access control measures as described in the configuration management documentation are effective in preventing unauthorised access to the configuration items. The developer's configuration management system was evaluated, and it was found to be consistent with the provided evidence.

25 The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of the TOE during distribution to the consumer.

2.1.2 Development

26 The evaluators analyzed the TOE functional specification; they determined that the design completely and accurately describes the TOE security functionality interfaces (TSFIs), and how the TOE security function (TSF) implements the security functional requirements (SFRs).

27 The evaluators examined the TOE design specification; they determined that the structure of the entire TOE is described in terms of subsystems. They also determined that, it provides a complete, accurate, and high-level description of the SFR-enforcing behavior of the SFR-enforcing subsystems.

28 The evaluators examined the TOE security architecture description; they determined that the information provided in the evidence is presented at a level of detail commensurate with the descriptions of the SFR-enforcing abstractions contained in the functional specification and TOE design.

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

2.1.3 Guidance documents

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

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

2.1.4 IT Product Testing

32 Testing at EAL 2 consists of assessing developer tests, performing independent functional test, and conducting penetration tests. The TOE testing was conducted by Securelytics SEF. 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 Assessment of Developer Tests

33 The evaluators verified that the developer has met their testing responsibilities by repeating some developer test, as documented in the Evaluation Technical Report (Ref [7]) (not a public document because it contains information proprietary to the developer and/or the evaluator). The results of the evaluators' tests are consistent with the developers' test results defined in their evaluation evidences submitted.

2.1.4.2 Independent Functional Testing

34 At EAL 2, independent functional testing is the evaluation conducted by evaluators 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 evaluators and are consistent with the expected test results in the test documentation.

Table 5: Independent Functional Test

Test ID	Description	Security Function	Results
F001 - Identification and Authentication	1. To test that the TOE maintains the following list of security attributes belonging to individual users (FIA_ATD.1): a) Email b) Password c) PIN Code 2. 2.To test that the TOE allows initiation of the activate account on behalf of the user (FIA_UAU.1). 3. 3.To test that the TOE requires each user to be successfully identified and authenticated before allowing any other TSF-mediated actions on behalf of that user (FIA_UAU.1, FIA_UAU.2 FIA_UID.2)	FIA_ATD.1 FIA_UAU.1 FIA_UAU.2 FIA_UID.2	Passed.
F002- Identification and Authentication Security Management	1. To test that the TOE provides a mechanism to verify that the secrets meet a minimum length of 8-characters (FIA_SOS.1) 2. 2. To test that the TOE restricts the ability to change the User Password/Admin Password to Authorised User and Admin (FMT_MTD.1)	FIA_SOS.1 FMT_MTD.1	Passed.
F003- Identification and Authentication	To test that the TOE re-authenticates the user if there is no user interaction over 30 minutes (FIA_UAU.6)	FIA_UAU.6	Passed.

Test ID	Description	Security Function	Results
F004 - Security Management	1. To test that the TOE enforces the access control SFP on objects and capable of performing the following management functions (FMT_SMF.1, FDP_ACC.1, FDP_ACF.1): 2. To test that the TOE enforces the access control SFP to restrict the ability to change, modify and delete the Admin Account, TOE Configuration, Users Account security attributes to Admin and Authorised User (FMT_MSA.1) 3. To test that the TOE enforces the access control SFP to provide restrictive default values for security attributes that are used to enforce the SFP (FMT_MSA.3) 4. To test that the TOE maintains the Authorised User and Admin user roles (FMT_SMR.1) 5. To test that the TOE able to associate users with roles (FMT_SMR.1) 6. To test that the TOE enforces the following rules to determine if an operation among controlled subjects and controlled objects is allowed (FDP_ACF.1): a. If the User is successfully authenticated accordingly, then access is granted based on privilege allocated; b. If the User is not authenticated successfully, therefore, access permission is denied	FMT_MSA.1 FMT_MSA.3 FMT_SMF.1 FMT_SMR.1 FDP_ACC.1 FDP_ACF.1	Passed.

Test ID	Description	Security Function	Results
F005 - Security Audit	1. To test that the TOE provides the Admin and Authorised User with the capability to read all audit information from the audit records (FAU_SAR.1) 2. To test that the TOE provides the audit records in a manner suitable for the user to interpret the information (FAU_SAR.1) 3. To test that the TOE able to generate an audit report of the following auditable events (FAU_GEN.1): a. Payment Transaction Status b. Bill Transaction Status c. Settlements Transaction Status d. User Signed In/ Signed Out e. Changes on user account 4. To test that the TOE records within each audit record at least the following information (FAU_GEN.1): a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event	FAU_SAR.1 FAU_GEN.1	Passed.
F006 - Secure Payment	1. To test that the TOE provides a communication path between itself and remote users or IT Systems that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure 2. To test that the TOE permits remote users to initiate communication via the trusted path	FTP_TRP.1	Passed.

Test ID	Description	Security Function	Results
	3. To test that the TOE requires the use of the trusted path for initial user authentication and all further communication after authentication		

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

2.1.4.3 Vulnerability Analysis

37 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.

38 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

2.1.4.4 Vulnerability testing

39 The penetration tests focused on:

a) Broken Access Control – Add Other's Product

b) Security Misconfiguration – Cookies

c) Parameter Tampering – Price Tampering

d) Modify Response – Use voucher on store with discount disable

e) Broken Access Control – Using Other User's Domain

f) Cross Site Scripting (XSS)

g) Broken Access Control – Add Same Domain

h) Input Validation

i) Insecure Direct Object Reference

j) SMS-based One Time Password (OTP) Reply

k) Registration Confirmation

l) Sensitive Information in Cookie

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]).

2.1.4.5 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 SecurePay Platform v4.9.1 which is performed by Securelytics SEF.

43 Securelytics SEF found that SecurePay Platform v4.9.1 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 2.

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 2 provides assurance by a full security target and analysis of the SFRs in that Security Target, using functional and interface specifications, guidance documentation and a description of the design of the TOE and the implementation to understand the security behaviours.

46 The analysis is supported by independent testing of the TSF, evidence of developer testing based on the functional specification, selective independent confirmation of the developer test results, and a vulnerability analysis (based upon the functional specification, TOE design, security architecture description and guidance evidence provided) demonstrating resistance to penetration attackers with a basic attack potential.

47 EAL 2 also provides assurance through use of a configuration management system and evidence of secure delivery procedures.

3.2 Recommendation

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

a) Developer is recommended to add ‘Delete’ operation for Admin role. The concern is if the Admin resigned, they still can access the system unless the resigned Admin is deleted.

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), v1, CyberSecurity Malaysia, December 2019.

[5] ISCB Evaluation Facility Manual (ISCB_EFM), v2a, August 2020.

[6] SecurePay Security Target, Version 1.0, 23 April 2021.

[7] Evaluation Technical Report, Version 1.0, 28 May 2021.

A.2 Terminology

A.2.1 Acronyms

Table 6: 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 7: 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 ---