MINISTRY OF COMMUNICATIONS
AND MULTIMEDIA MALAYSIA

CyberSecurity MALAYSIA

C100 Certification Report

Fortix Security Suite version 1.17.1

File name: ISCB-3-RPT-C100-CR-v1
Version: v1
Date of document: 23 May 2019
Document classification: PUBLIC

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

CyberSecurity Malaysia
(726630-U)
T +603 8800 7999
F +603 8008 7000
H 1 300 88 2999

Corporate Office:
Level 7, Tower 1
Menara Cyber Axis
Jalan Impact
63000 Cyberjaya
Selangor Darul Ehsan
Malaysia.
www.cybersecurity.my

C100 Certification Report

Fortix Security Suite version 1.17.1

23 May 2019

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:	C100 Certification Report
DOCUMENT REFERENCE:	ISCB-3-RPT-C100-CR-v1
ISSUE:	v1
DATE:	23 May 2019

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. 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 17th June 2019, 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	9 May 2019	All	Initial draft
v1	23 May 2019	All	Final version

Executive Summary

The Target of Evaluation (TOE) is the Fortix Security Suite version 1.17.1. The TOE is a web application and web services to support secure delivery of PIN to customers and secure data communication between endpoints.

Fortix Security Suite consists of Secure ePin module and WebSeal module which is hosted in SafeNet Java Hardware Security Module (HSM).

The Secure ePin module provides PIN delivery using split-channel delivery regardless of customers' locations at any time. This service is typically used for delivering credit cards PIN or sensitive authentication PIN. Customers will receive their PINs that are embedded inside an encrypted PDF document via their emails along with a SMS notification which contains a password to the PDF document.

The WebSeal module (Secure End-to-End encryption) helps application to achieve a true end-to-end encryption, from the web browser/mobile application to the web server or application server, and database server, offering a level of security unavailable from software alternatives to support critical business processes. WebSeal ensures that no sensitive data is accessible in clear while travelling over the network throughout an application's operation cycles. Seeding of E2EE JavaScript is performed here.

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 Across Verticals lab and the evaluation was completed on 9 May 2019.

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 Fortix Security Suite version 1.17.1 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 decide 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 a web application and web services to support secure delivery of PIN to customers and secure data communication between endpoints.

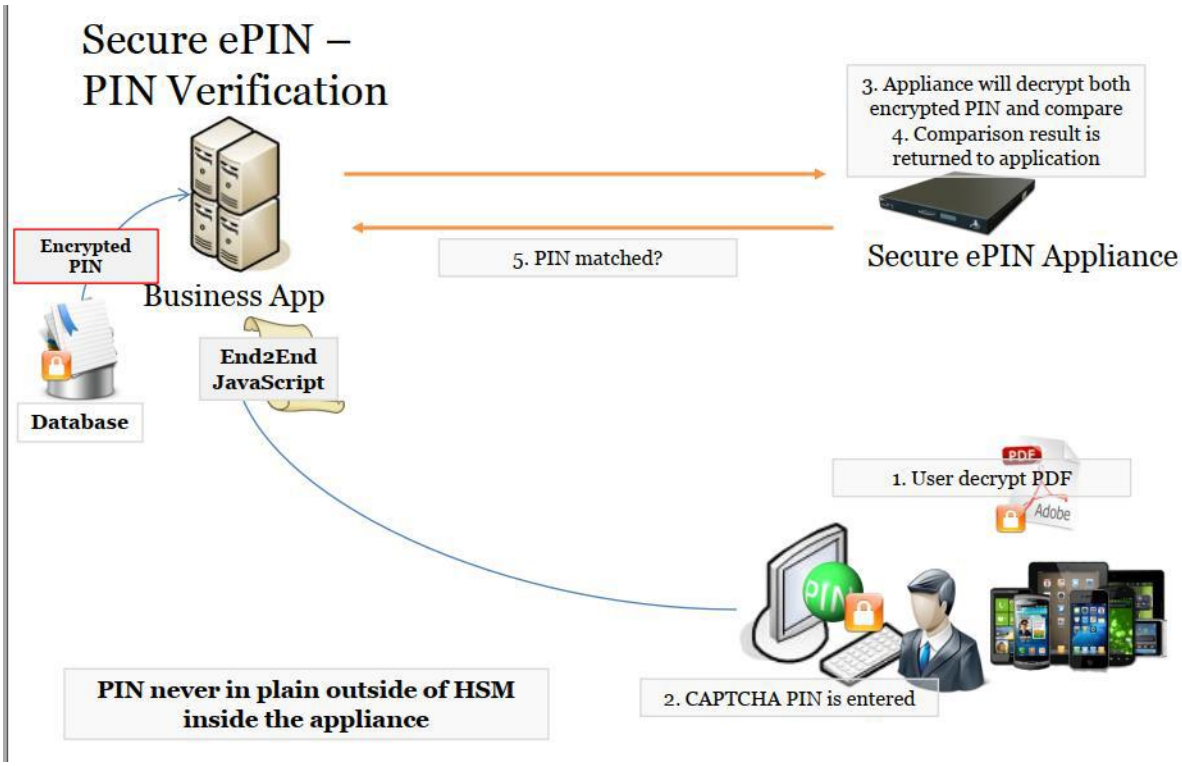
2 Fortix Security Suite consists of the Secure ePin module and WebSeal module which is hosted in SafeNet Java Hardware Security Module (HSM).

3 The Secure ePin modules provides PIN delivery using split-channel delivery regardless of customers' locations at any time. This service is typically used for delivering credit cards PIN or sensitive authentication PIN. Customers will receive their PINs that are embedded inside an encrypted PDF document via their emails along with a SMS notification which contains a password to the PDF document.

4 The WebSeal module (Secure End-to-End encryption) helps application to achieve a true end-to-end encryption, from the web browser/mobile application to the web server or application server, and database server, offering a level of security unavailable from software alternatives to support critical business processes. WebSeal ensures that no sensitive data is accessible in clear while travelling over the network throughout an application's operation cycles. Seeding of E2EE JavaScript is performed here.

5 One common use case is that after the customer received the authentication PIN from Secure ePIn. WebSeal will be leveraged to encrypt the PIN and sent back to the business application as in Figure 1.

Figure 1: Fortix Security Suite Common Use Case



6 The major security features of the TOE included:

a) Identification and authentication

b) User data protection

c) Security management

d) TOE access

e) Security Audit

1.2 TOE Identification

7 The details of the TOE are identified in Table 1 below.

Table 1: TOE identification

Evaluation Scheme	Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme
Project Identifier	C100
TOE Name	Fortix Security Suite
TOE Version	1.17.1
Security Target Title	Fortix Security Suite Security Target
Security Target Version	0.5
Security Target Date	4 April 2019
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
Sponsor	Blue Fortress Sdn Bhd Unit 05-06, Level 5, Tower B, Vertical Business Suite, Avenue 3, No. 8, Jalan Kerinchi, Bangsar South, 59200 Kuala Lumpur
Developer	Blue Fortress Sdn Bhd Unit 05-06, Level 5, Tower B, Vertical Business Suite, Avenue 3, No. 8, Jalan Kerinchi, Bangsar South, 59200 Kuala Lumpur
Evaluation Facility	Across Vertical Lab

1.3 Security Policy

8 No organisational security policies have been defined regarding the use of the TOE.

1.4 TOE Architecture

9 The TOE includes both physical and logical boundaries which are described in Section 1.5 of the Security Target (Ref [6]).

1.4.1 Logical Boundaries

10 The scope of the evaluation was limited to those claims made in the Security Target (Ref [6]) and includes only the following evaluated security functionality:

a) Identification and Authentication

TOE shall allow System Initialization before Root Admin being identified and authenticated. Root Admin, System Admin and System Operator can be authenticated using login ID and password at the TOE Management Console. Web Services user (node) can be authenticated using login ID and password when calling web services.

- TOE shall reauthenticate the Root Administrator, System Administrator and System Operator if idle for 10 minutes on the Web Management Console; TOE shall reauthenticate the Web Services User if idle for 30 minutes after authentication through calling web services API.
- TOE shall maintain several security attributes belonging to individual users.

b) Security Management

There are several roles maintained in TOE: Root Admin, System Admin, System Operator and Web Services user.

The TOE is able to perform several management functions as following:

a. System Initialization

b. HSM Storage Cleanup

c. Backup Database

d. Restore Database

e. SMTP Configuration

f. SMS Configuration

g. SMS Provider Configuration

h. Email Template Management

i. PIN Mailer Template Management

j. Key Import

k. Generate Keypairs

l. Decimalization Table

m. User Management

n. View System Log

o. Node Management

p. Change Own Password

Web Services user does not have management role. Download App Log is not part of the scope.

The authorized roles are able to modify, delete and add TSF data for each management functions mentioned above.

When a new node is added, it will have the “Restricted” state. Root Admin, System Admin, System Operator are able to change default value for Node Management from “ Restricted” to “Granted”.

c) User Data Protection

TOE shall enforce Access Control Policy to control user access on TOE Management Console functions according to their roles. Different roles will obtain different access functions in the Management Console. Additionally, a business application endpoint is able to use WebSeal End2End JavaScript to encrypt/decrypt data provided by user to be sent the Internet to itself.

TOE shall also enforce Secure ePIN Policy in generating/converting PIN in CAPTCHA format to be embedded in encrypted PDF file.

PDF file will be sent to customer in email and password of the PDF file will be sent using SMS.

However, true random number generation and encryption are executed by HSM which are not part of the scope. Security attributes shall be used in order to enforce Access Control Policy and Secure ePIN Policy. Secure ePIN Policy shall be enforced when exporting PIN to the intended user.

d) TOE Access

User will also be denied establishing a session with the TOE if the client did not present a valid certificate for client-side authentication. Additionally, only nodes that have their source IP Address whitelisted can call the web services.

e) Security Audit

TOE shall be able to generate audit record for several auditable events. Each event will be recorded with date and time, type of event, subject identity and outcome of the event. However, the timestamp for the audit record is provided by the HSM operating system, which is not part of the scope.

Audit records can be reviewed by Root Admin, System Admin and System Operator in a suitable manner.

TOE shall protect the audit records from unauthorized deletion or modification.

f) Trusted Channels

TOE shall provide a secure communication channel between WebSeal Module to business application and HSM. Any data transferred between this channels will be in encrypted format to protect from modification and disclosure.

1.4.2 Physical Boundaries

11 The guidance document is delivered together with the TOE separate media support, the TOE on separate media support, which means that the TOE (Physical HSM with the TOE installed) will be delivered physically, and PDF guidance documents will be delivered through the internet logically (e.g Email/Support portal) in order to support the administrator and user in administrating and operating the TOE.

1.5 Clarification of Scope

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

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

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

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

1.6.1 Environmental assumptions

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

a) A.ENV

The TOE environment is physically and logically secure.

b) A.STORAGE

THE PIN will be stored securely in TOE environment.

c) A.ENCRYPT

The TOE environment will encrypt PDF file securely.

d) A.KEYGEN

The TOE environment will generate and manage the true random number and encryption key securely.

e) A.SMS

The TOE environment for SMS delivery is secure.

f) A.ADMIN

The Administrator for the environment will be non-hostile and follows guidance documentation accordingly; however, the Administrator is not free from human error and mistakes.

1.7 Evaluated Configuration

1.7.1 Domain Separation

17 The TOE does not provide security domains to potentially-harmful entities. The TOE relies on the operational environment which is the Safenet Luna SP HSM to provide the

domain separation. The TOE management functionality described does not provide security domains, but is a direct implementation of the security requirements. In short, security domains are not applicable for this TOE.

1.7.2 Initialisation

18 After the TOE securely delivered to the customer, the TOE will be in inactive state where its configurations are not yet configured. User needs to first boot up the TOE by accessing the Management Console through web browser. During the initialization, the first or default user called “root” with Root Admin role will be created. User need to create a password for user “root”.

Root Admin shall then login to the Management Console as user “root” and create the first operational admin, either System Admin or System Operator. System Admin and System Operator are enforced to change their default password during first time login to avoid unauthorized authentication by impostor. Only then the TOE will be in its initial secure state.

User certificate is needed by the Root Admin, System Admin, and System Operator for session establishment. For the web services user, the web services user (node) calling the API must be in GRANTED state first. No need for Web Services User to have a user certificate.

Administrators shall access the TOE using web browser by accessing the configured IP address with the default port in the HSM and provide their username and password to login to the TOE.

1.7.3 Protection from Tampering

1.7.3.1 Physical Protection

19 HSM appliance sealed with a security tape at the casing to avoid product being tampered during distribution to the customer. If the security tape is broken, unauthorized person may have tampered the TOE.

20 HSM appliance shall be located in a physically secure facility to ensure unauthorized access prevented.

1.7.3.2 Logical

21 The TOE is administered through web browser by accessing the Management Console.

User's username and user certificate is enforced by the TOE to protect unauthorized user from accessing the TOE from HTTP connection. If someone sniffed the network, the attacker could only obtain the ciphertext of the communication.

TOE consist of WebSeal End-to-End Encryption (E2EE) module which provides a JCE library with custom API's for developers to perform an end-to-end encryption/decryption. If someone sniffed the network, the attacker could only obtain the ciphertext of the communication.
For PDF which will be sent out via SMTP gateway, the PDF will be encrypted with random number from true random number generator of the HSM. The encryption is according to PDF ISO 32000-1. Default encryption algorithm is AC4-128bits encryption. AES 128 and 256 is supported however that requires the customer to have Acrobat Reader version 9 and above installed to be able to open the PDF.
Web service user password is not sent across the network. Password is hashed locally and the result of the hashing with given salt is sent to Secure ePIN for verification. Although system is designed as such, it is still advisable to send the data via SSL/TLS/HTTPS to have maximum protection for data in transit.

22 The Secure ePIN when running in the HSM will only have limited business web services call. It will not have low level HSM functions such as decrypt particular data and return plain data etc. It will only accept a PIN offset and split out an encrypted PDF file and encrypted data if there is any.

1.7.4 Protection from Bypassing

23 TSF ensures that the security functionality is always invoked with the self-protection (as described earlier in this document) and correct functional behaviour (as described in the FSP/TDS/ATE evaluation evidence).

TOE is not bypassable dependent on functionality in the HSM. HSM will only allow digitally signed application to be run inside the HSM appliance.

The TOE allow both Secure ePIN PDF and PDF decryption password to be returned to caller application, it is not a good practice to configure as such. The Secure ePIN generated in CAPTCHA format inside the PDF will be at risk since all elements to open up the encrypted Secure ePIN is available to caller application.

1.8 Delivery Procedures

24 The evaluators examined the delivery procedure, in which provide guidance for the developer to initiate delivery process of the TOE and its components to the intended recipient(s). It is also provide direction on the methods used to deliver the TOE to consumers and users of the product.

25 The customer will purchase the product and complete the payment. Once payment is confirmed and legal documentations have been completed, Blue Fortress personnel can proceed with preparing the product.

26 Blue Fortress personnel will make the necessary preparation:

a) Prepare the Fortix Security Suite Administrator Guide and Developer Guide for Fortix Security Suite and deliver to the customer by E-mail

b) Prepare the installer package for Fortix Security Suite

c) Fortix Security Suite application shall be digitally signed to be run inside the HSM appliance

d) Install and configure the Fortix Security Suite application in the HSM appliance

e) Check TOE version on the Fortix Security Suite web console login page.

27 The product will be hand-delivered to customer.

28 Once the package is delivered, the customer is expected to perform the following measures:

a) Receive the package.

b) Acknowledge received items receipt as per Appendix A of Fortix Security Suite Delivery Procedure Document.

29 Blue Fortress personnel will keep the Acknowledge received items as proof of product receipt. Customer is expected to use the *Fortix Security Suite Administrator Guide*. For application developer, they can use *Fortix Security Suite Developer Guide* to integrate their application with Fortix Security Suite. Customer acceptance of product will be based verification of functionalities as per the *Administrator Guide.*

2 Evaluation

30 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 ISCB Product Certification Schemes Policy (Product_SP) (Ref [4]) and ISCB Evaluation Facility Manual (ISCB_EFM) (Ref [5]).

2.1 Evaluation Analysis Activities

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

2.1.1 Life-cycle support

32 The evaluators checked that the TOE provided for evaluation is labelled with its reference.

33 The evaluators checked that the TOE references used are consistent.

34 The evaluators examined the method of identifying configuration items to determine that it describes how configuration items are uniquely identified.

35 The evaluators examined the configuration items to determine that they are identified in a way that is consistent with the CM documentation.

36 The evaluators checked that the configuration list includes the

a) the TOE itself;

b) the parts that comprise the TOE;

c) the evaluation evidence required by the SARs

37 The evaluators examined the configuration list to determine that it uniquely identifies each configuration item.

38 The evaluators checked that the configuration list indicates the developer of each TSF relevant configuration item.

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

40 The evaluators examined aspects of the delivery process to determine that the delivery procedures are used.

41 Evaluators confirmed that all the requirements in this class were fulfilled and passed.

2.1.2 Development

42 The evaluators assessed the requirements of the ADV class for an EAL 2 evaluation level of the TOE.

43 The evaluators examined the functional specification to determine that the TSF is fully represented, it states the purpose of each TSFI and the method of use for each TSFI is given.

44 The evaluators examined the presentation of the TSFI to determine that it completely identifies all parameters associated with every TSFI.

45 The evaluators examined the presentation of the TSFI to determine that it completely and accurately describes all parameters associated with every TSFI.

46 The evaluators examined the presentation of the TSFI to determine that it completely and accurately describes the SFR-enforcing actions associated with the SFR-enforcing TSFIs.

47 The evaluators examined the presentation of the TSFI to determine that it completely and accurately describes error messages that may result from SFR-enforcing actions associated with each SFR-enforcing TSFI.

48 The evaluators checked that the tracing links the SFRs to the corresponding TSFIs.

49 The evaluators examined the functional specification to determine that it is a complete and accurate instantiation of the SFRs

50 The evaluators examined the security architecture description to determine 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 document.

51 The evaluators examined the security architecture description to determine that it describes the security domains maintained by the TSF.

52 The evaluators examined the security architecture description to determine that the initialisation process preserves security.

53 The evaluators examined the security architecture description to determine that it contains information sufficient to support a determination that the TSF is able to protect itself from tampering by untrusted active entities.

54 The evaluators examined the security architecture description to determine that it presents an analysis that adequately describes how the SFR-enforcing mechanisms cannot be bypassed.

55 The evaluators examined the TOE design to determine that the structure of the entire TOE is described in terms of subsystems and all subsystems of the TSF are identified.

56 The evaluators examined the TOE design to determine that each SFR-supporting or SFR-non-interfering subsystem of the TSF is described such that the evaluator can determine that the subsystem is SFR-supporting or SFR-non-interfering.

57 The evaluators examined the TOE design to determine that it provides a complete, accurate, and high-level description of the SFR-enforcing behaviour of the SFR-enforcing subsystems.

58 The evaluators examined the TOE design to determine that interactions between the subsystems of the TSF are described.

59 The evaluators examined the TOE design to determine that it contains a complete and accurate mapping from the TSFI described in the functional specification to the subsystems of the TSF described in the TOE design.

60 The evaluators examined the TOE security functional requirements and the TOE design, to determine that all ST security functional requirements are covered by the TOE design.

61 The evaluators examined the TOE design to determine that it is an accurate instantiation of all security functional requirements.

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

2.1.3 Guidance documents

63 The evaluators analyzed the TOE guidance documentation for secure preparation and installation of the TOE, and the guides for secure operation, provided in Fortix Security Suite installation Guide (Ref [8]).

64 Evaluator examined operational user guidance and preparative procedures.

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

2.1.4 IT Product Testing

66 Testing at EAL 2 consists of assessing developer tests, sufficiency test and conducting penetration tests. The TOE testing was conducted by evaluators from Across Vertical lab. 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

67 The evaluators verified that the developer has met their testing responsibilities by repeating all the 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 Test

68 At EAL 2, independent test demonstrates the correspondence between the security functional requirements (SFRs) defined in Security Target, and the test cases that test the functions and behaviour of the TOE that meets those requirements. The evaluators have decided to perform testing based on the TOE Security Functions.

69 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 developed and performed by the evaluators to verify the functionality as follows:

Table 2: Independent Test

Test ID	Description	Results
FSSCC005-F001	To ensure that TSF allow System Initialization on behalf of the user to be performed before the user is identified and authenticated and require each user to be successfully identified and authenticated before allowing any other TSF-mediated actions on behalf of that user.	Pass
FSSCC005-F002	To ensure that the TSF is capable of performing the following management functions: • System Initialization • Reinitialize System • Clean Up • Backup Database • Restore Database • Change Password • User Management • Node Management • View System Log • SMTP Configuration • SMS Configuration • SMS Provider Configuration • Email Template Configuration • PIN Mailer Template Configuration • Import Key • Decimalization Table Configuration	Pass
FSSCC005-F003	This test ensures that the TSF maintain the following list of security attributes belonging to individual users: • Login ID • Password • Role This test also verifies that the TSF maintain 4 roles, which are: • Root Admin • System Admin • Operator Admin • Web Services User	Pass
FSSCC005-F004	To ensure that the TSF enforce the access control policy to provide restrictive default values for security attributes that are used to enforce the SFP. The TSF shall allow Root Admin, System Admin and System Operator to specify alternative initial values to override the default values when an object or information is created.	Pass

Test ID	Description	Results
FSSCC005-F005	To ensure that the TOE require user to be re-authenticated under the condition user did not perform any actions for 10 minutes after session establishment with TOE.	Pass
FSSCC005-F006	To ensure the TSF will deny session establishment based on user personal authentication certificate and IP address.	Pass
FSSCC005-F007	To ensure the access control policy and restriction on the user ability based is on the role privilege.	Pass
FSSCC005-F008	To ensure that the TSF ensure web service user is authenticate, authorize and the user pin is generated in an encrypted PDF file with CAPTCHA format and password to decrypt the PDF file is embedded in the SMS.	Pass
FSSCC005-F009	To ensure that the TSF explicitly authorize access of subjects to objects based on the following additional rules: The first user that access the TOE after TOE first time start-up have the ability to initialize the system by setting up the root account and explicitly deny access of subjects to objects based on the following additional rules: no subjects may delete the account of root admin.	Pass
FSSCC005-F010	To ensure that the TSF shall capable to generate meaningful message in the log with accurate timestamp and allow the log file to be available for those user roles which have the privilege. Log integrity must also be maintained as no modification on the log is allowed.	Pass
FSSCC005-F011	To ensure the data that send out of from the client browser all the way to the HSM is in encrypted format and only able to decrypt inside the HSM or by the E2EE JavaScript which embedded in the business application.	Pass

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

2.1.4.3 Vulnerability Analysis

71 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.

72 From the vulnerability analysis, the evaluators conducted penetration testing to determine that the TOE is resistant to attacks 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 (elapse 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) Equipment

2.1.4.3.1 Vulnerability testing

73 The penetration tests focused on:

a) Injection

b) Broken Authentication

c) Sensitive Data Exposure

d) Broken Access Control

e) Security Misconfiguration

f) Cross-Site Scripting (XSS)

g) Using Components with Known Vulnerabilities

h) Insufficient Logging & Monitoring

74 The results of the penetration testing demonstrate that the TOE is resistant to an attacker possessing a high attack potential. However, it is important to ensure that the TOE is use only in its evaluated configuration and in a secure environment as specified in the Security Target (Ref [6]).

2.1.4.4 Testing Results

75 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

76 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 Fortix Security Suite version 1.17.1 which is performed by Across Vertical lab.

77 Across Vertical lab found that Fortix Security Suite version 1.17.1 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.

78 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

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

80 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 an attacker possessing a Basic attack potential.

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

3.2 Recommendation

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

a) The TOE users to keep on updating, maintaining, backing up configuration, logs and related data/files of the TOE, auditing the security enforcing rules of the TOE and performing checks on the TOE regularly to maintain its secure operational environment
b) A strict adherence to guidance documentations and procedures provided by the developer are highly recommended.

c) The TOE users should be aware and implement available security or critical updates related to the TOE security features and its supporting hardware, software, firmware or relevant guidance documents.
d) Users are advice to seek assistance or guidance directly from the developer of the TOE if specific requirements shall be configured or implemented by the TOE to meet certain policies, procedures and security enforcement within the users' organisation. This is important in order to reduce operational error, misconfiguration, malfunctions or insecure operations of the TOE that may compromise the confidentiality, integrity and availability of the assets that is protected by the TOE.

Annex A References

A.1 References

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

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

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

[4] ISCB Product Certification Schemes Policy (Product_SP), v1b, CyberSecurity Malaysia, March 2018.

[5] ISCB Evaluation Facility Manual (ISCB_EFM), v1a, March 2018.

[6] Fortix Security Suite v.1.17.1, Version 0.5, 4 April 2019.

[7] Evaluation Technical Report Version 2.0, 7 May 2019.

[8] Fortix Security Suite Installation Guide, Version 0.2, July 2018.

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
MyCC	Malaysian Common Criteria Evaluation and Certification Scheme
MyCPR	MyCC Scheme Certified Products Register
MySEF	Malaysian Security Evaluation Facility
PP	Protection Profile

Acronym	Expanded Term
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
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.

Term	Definition and Source
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 ---