CyberSecurity
MALAYSIA
An agency under MOSTI

C064 Certification Report

SecureMi® v1.2

File name: ISCB-5-RPT-C064-CR-v1
Version: v1
Date of document: 6 September 2017
Document classification: PUBLIC

Malaysian Common Criteria Evaluation & Certification Scheme

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

Securing Our Cyberspace

CyberSecurity Malaysia

T +603 8992 6888
F +603 8992 6841
H 1 300 88 2999

Corporate Office
Level 5, Sapura@Mines
No 7, Jalan Tasik
The Mines Resort City
43300 Seri Kembangan
Selangor Darul Ehsan
Malaysia.

www.cybersecurity.my

C064 Certification Report

SecureMi® v1.2

6 September 2017
ISCB Department

CyberSecurity Malaysia
Level 5, Sapura@Mines,
No 7 Jalan Tasik, The Mines Resort City
43300 Seri Kembangan, Selangor, Malaysia
Tel: +603 8992 6888 · Fax: +603 8992 6841
http://www.cybersecurity.my

Document Authorisation

DOCUMENT TITLE:	C064 Certification Report
DOCUMENT REFERENCE:	ISCB-5-RPT-C064-CR-v1
ISSUE:	v1
DATE:	6 September 2017

DISTRIBUTION:	UNCONTROLLED COPY - FOR UNLIMITED USE AND DISTRIBUTION

Copyright Statement

Registered office:
Level 5, Sapura@Mines,
No 7 Jalan Tasik,
The Mines Resort City,
43300 Seri Kembangan
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 6 September 2017, 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).

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

Disclaimer

The Information Technology (IT) product identified in this certification report and its associated certificate has been evaluated at an accredited and licensed evaluation facility established under the Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme (Ref [4]) using the Common Methodology for IT Security Evaluation, version 3.1 revision 4 (Ref [3]), for conformance to the Common Criteria for IT Security Evaluation, version 3.1 revision 4 (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	16 August 2017	All	Initial draft of certification report
v1	28 August 2017	All	Final version of certification report

Executive Summary

SecureMi® is the Target of Evaluation (TOE) for the Common Criteria Evaluation Assurance Level 2 evaluation. The TOE (SecureMi®) is a content aware **Data Leakage Prevention (DLP**) solution that is designed as a complete solution for preventing data leakage problems in government and corporate environments. It has the capabilities to detect and prevent any unauthorized use and transmission of confidential information in an organization by insiders. It consists of policies, procedures, and technical controls that will be defined by organization's team members on a centralized management framework. It provides capabilities to classify, discover, monitor, and protect data in use, data in motion, and data at rest through detection procedures using content pattern matching techniques. The TOE then takes actions based on pre-defined policies to protect the information from leakage and misuse.

There are 3 components comprising the TOE; SecureMi® Centralized Management Console (CMC), SecureMi® Storage, and SecureMi® Endpoint. The SecureMi® Centralized Management Console (CMC) is web application that provides administrative access. The SecureMi® Storage and SecureMi® Endpoint provide the sensitive data protection through content analysis on documents and transmissions using a shared, policy-driven engine.

The scope of evaluation covers major security features as follows:

a) **Security Audit**: The Security Audit function of the TOE provides functionality for generation and viewing of audit data. Authorized officers can view audit log entries captured by the TOE through SecureMi® CMC as the audit logs captured by SecureMi® Endpoint and SecureMi® Storage are forwarded to the SecureMi® CMC where they can be viewed through the SecureMi® CMC GUI.

b) **Identification & Authentication**: Authorized officers must be identified and authenticated before they can perform any management tasks on the TOE or TOE data. Authorized officers authenticate to the SecureMi® CMC with a user ID and password through a web browser. Once authorized officers are authenticated, they may perform management tasks as allowed by their permissions.

c) **Security Management**: Security Management functions define roles and role management functionality of the TOE. By default, the TOE comes with a few authorized officer roles such as Policy Manager, Incident Manager, Administrator and Super Administrator. The Super Administrator role can define one or more Limited authorized officer roles (such as default roles, Policy Manager, Incident Manager and Administrator), and assign permissions to them as appropriate. Each authorized officer is also assigned a user group and user ID, which help to further define the permissions granted. Alternative default values may be specified by the Super Administrator.

d) **User Data Protection**: The TOE allows authorized officers to enforce a rigid Administrative Access Control Rules and Policies for authorized officers accessing the TOE. The TOE enforces authorized officer-configurable policies on access to sensitive data:

SecureMi® Endpoint requires the end-users to key-in a correct OTP to retrieve quarantined data on targeted machines.

Data Discovery Policies enforce rules governing the suitability of files on targeted machines to store sensitive data.

SecureMi® Endpoint provides a secure vault for end-users to store sensitive data.

This report confirms the findings of the security evaluation of the TOE to the Common Criteria (CC) Evaluation Assurance Level 2 (EAL2) was conducted in accordance with the relevant criteria and the requirements of the Malaysia Common Criteria Evaluation and Certification (MyCC) Scheme (Ref [4]).

The evaluation was performed by CyberSecurity MySEF (Malaysia Security Evaluation Facility) and completed on 14 August 2017.

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 www.cybersecurity.my/mycc and the Common Criteria portal (the official website of the Common Criteria Recognition Arrangement) at www.commoncriteriaportal.org.

It is the responsibility of the user to ensure that SecureMi® v1.2 meets their requirements. It is recommended that a potential user of SecureMi® v1.2 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

1 Target of Evaluation

1.1 TOE Description

1 The Target of Evaluation (TOE) is a content aware **Data Leakage Prevention (DLP**) solution that is designed as a complete solution for preventing data leakage problems in government and corporate environments from the start. It has the capabilities to detect and prevent any unauthorized use and transmission of confidential information of an organization by insiders. It consists of policies, procedures, and technical controls that will be defined by the organization's team members on a centralized management framework. It is capable of classifying, discovering, monitoring, and protecting data in use, data in motion, and data at rest through detection procedures using content pattern matching techniques. The TOE then takes actions based on pre-defined policies to protect the information from leakage and misuse.

2 There are 3 components within the TOE; SecureMi® Centralized Management Console (CMC), SecureMi® Storage, and SecureMi® Endpoint.

3 The SecureMi® Centralized Management Console (CMC) is web application that provides administrative access.

4 The SecureMi® Storage and SecureMi® Endpoint provide sensitive data protection through content analysis on documents and transmissions using a shared, policy-driven engine.

Subsystems	Overview
SecureMi® Centralized Management Console (SecureMi® CMC)	SecureMi® CMC is a web application with which an authorized officer configures and manages all the other DLP products. SecureMi® CMC is accessed through a standard web browser over HTTPS (CMC GUI). Each installation of DLP products typically includes only one instance of SecureMi® CMC. SecureMi® CMC requires a database, called the SecureMi® CMC Database (not included in scope of evaluation), for storing the configurations, security policies, and the results of analyses performed by the other components. SecureMi® CMC is the primary interface to the SecureMi® Endpoint Services. For every service offered there is at least one corresponding set of functions that enable operators to invoke that service.
SecureMi® Storage	SecureMi® Storage is a software agent that install on together with SecureMi® CMC on the same machine. It is a software service that starts when the computer starts and has a system tray icon on server and provides Graphical User Interface (Storage GUI) for authorized officers to retrieve quarantined documents from data discovery scanning. Authorized officers can enlist an unlimited number of files on SecureMi® CMC to be tagged as sensitive data in the system. Once the source path and the schedule to scan is defined,

	SecureMi® Storage will automatically classify the files so that these fingerprints can be used to identify confidential data elsewhere.
SecureMi® Endpoint	The SecureMi® Endpoint is a software service that starts when the computer starts, and monitors end-user actions as long as the computer is running. SecureMi® Endpoint runs from within the targeted machine's operating system, and are transparent to desktop applications. The SecureMi® Endpoint injects itself into each running process on the targeted machine, and intercepts and monitors application calls. When an application call for an end-user action such as copy, move, or print is intercepted, the SecureMi® Endpoint extracts the content of the document involved, and performs an analysis on the content to determine if a policy violation has occurred. If so, the SecureMi® Endpoint performs the necessary actions based on the policy retrieved earlier from SecureMi® CMC. SecureMi® Endpoint consists of five subsystems: SecureMi® Endpoint Super Agent, SecureMi® Endpoint Agent, SecureMi® Endpoint Policy Manager, SecureMi® Endpoint Service and SecureMi® Endpoint Bridge Service.

5 The details of TOE security functions can be found in section 2.2 of the Security Target (Ref[6])

6 There are four (4) security functionalities covered under the scope of evaluation which are:

Security Function	Description
Security Audit	The Security Audit function provides the TOE with the functionality for generation and viewing of audit data. Authorized officers can view audit log entries captured by TOE through SecureMi® CMC as the audit logs captured by SecureMi® Endpoint and SecureMi® Storage are forwarded to the SecureMi® CMC where they can be viewed through the CMC GUI.
Identification and Authentication	Authorized officers must be identified and authenticated before they can perform any management tasks on the TOE or TOE data. Authorized officers authenticate to the SecureMi® CMC with a user ID and password through a web browser. Once authorized officers are authenticated, they may perform management tasks as allowed by their permissions.
Security Management	Security Management functions define roles and role management functionality of the TOE. By default, the TOE comes with a few

	authorized officer roles such as Policy Manager, Incident Manager, Administrator and Super Administrator. The Super Administrator role can define one or more Limited authorized officer roles (such as default roles, Policy Manager, Incident Manager and Administrator), and assign permissions to them as appropriate. Each authorized officer is also assigned a user group and user ID, which help to further define the permissions granted. Alternative default values may be specified by the Super Administrator.
User Data Protection	The TOE allows authorized officers to enforce a rigid Administrative Access Control Rules and Policies for authorized officers accessing the TOE. The TOE enforces authorized officer-configurable policies on access to sensitive data: SecureMi® Endpoint requires the end-users to key-in a correct OTP to retrieve quarantined data on targeted machines. Data Discovery Policies enforce rules governing the suitability of files on targeted machines to store sensitive data. SecureMi® Endpoint provides a secure vault for end-users to store sensitive data.

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	C064
TOE Name	SecureMi®
TOE Version	V1.2
Security Target Title	SecureMi® Version 1.2 Security Target
Security Target Version	0.13
Security Target Date	4 July 2017
Assurance Level	Evaluation Assurance Level 2 (EAL2)
Criteria	Common Criteria for Information Technology Security Evaluation, September 2012, Version 3.1 Revision 4 (Ref [2])

Methodology	Common Evaluation Methodology for Information Technology Security Evaluation, September 2012, Version 3.1 Revision 4 (Ref [3])
Protection Profile Conformance	None
Common Criteria Conformance	CC Part 2 Conformant CC Part 3 Conformant
Sponsor and Developer	Evault Technologies Sdn Bhd 1st Floor Block G, Excella Business Park Jalan Ampang Putra, Taman Ampang Hilir 55100 Kuala Lumpur
Evaluation Facility	CyberSecurity MySEF

1.3 Security Policy

8 There are five (5) organisational security policies that have been defined regarding the use of the TOE.

OSP	Description
P.AUDIT	The TOE shall generate and maintain a record of security-related events to ensure accountability. Records shall be reviewed based on the timeline defined by the organizational audit process and procedures.
P.SECUREMGMT	Knowledgeable and competent TOE authorized officer/s shall be assigned to manage the TOE securely and keep the TSF data up to date.
P.STATISTICS	TOE authorized officer/s shall record, analyze and produce statistics on the data of audit and incident. TOE shall have reporting capabilities built-in inside or integrate with other authorized software/system to generate eligible reports.
P.INTERTRUSTEDCHANNEL	The TOE environment shall support inter-trusted channel (secure platform) to establish a secure communication among trusted IT entities.
P.POLICIES	The organization has in place policies and procedures to prevent unauthorized access to the TOE and its underlying environment.

1.4 TOE Architecture

9 The TOE includes both logical and physical boundaries, which are described in Section 2.3 of the Security Target (Ref [6]).

10 The following figure 1 shows the evaluated configuration that comprise the TOE:

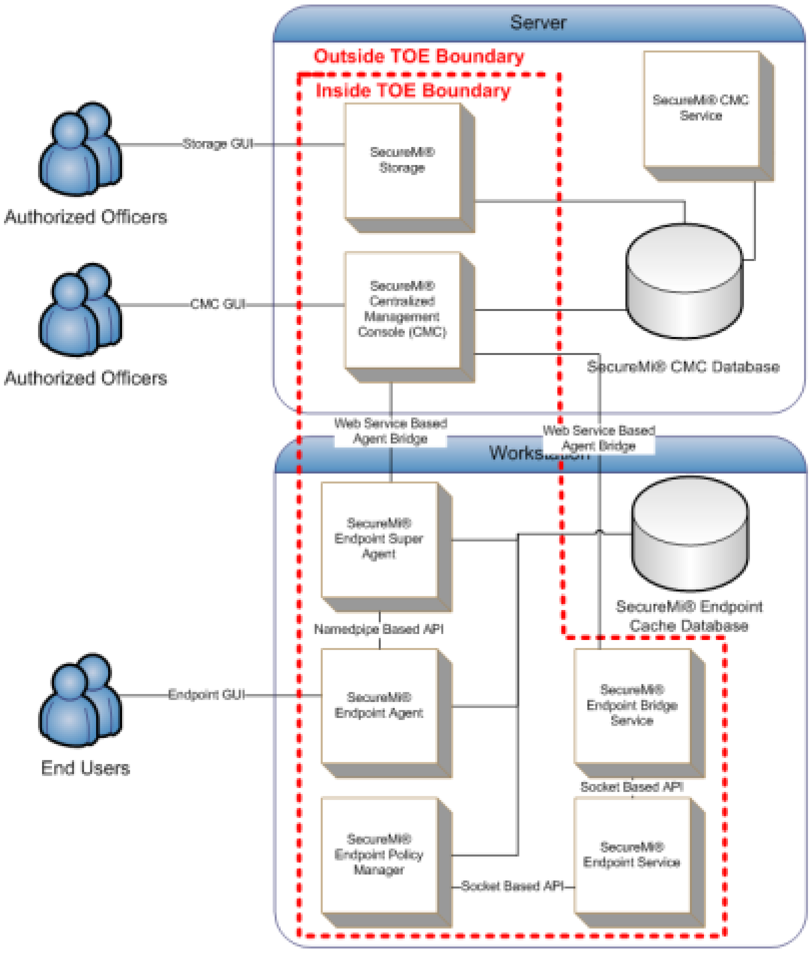

Figure 1: TOE boundary and subsystems

1.4.1 Logical Boundaries

11 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) Security Audit: The Security Audit function provides the TOE with the functionality for generation and viewing of audit data. Authorized officers can view audit log entries captured by the TOE through SecureMi® CMC as the audit logs captured by SecureMi® Endpoint and SecureMi® Storage are forwarded to the SecureMi® CMC where they can be viewed through the CMC GUI.

b) Identification and Authentication: Authorized officers must be identified and authenticated before they can perform any management tasks on the TOE or TOE data. Authorized officers authenticate to the SecureMi® CMC with a user ID and password through a web browser. Once authorized officers are authenticated, they may perform management tasks as allowed by their permissions.

c) Security Management: Security Management functions define roles and role management functionality of the TOE. By default, the TOE comes with a few authorized officer roles such as Policy Manager, Incident Manager, Administrator and Super Administrator.
The Super Administrator role can define one or more Limited authorized officer roles (such as default roles, Policy Manager, Incident Manager and Administrator), and assign permissions to them as appropriate. Each authorized officer is also assigned a user group and user ID, which help to further define the permissions granted. Alternative default values may be specified by the Super Administrator.

d) User Data Protection: The TOE allows authorized officers to enforce a rigid Administrative Access Control Rules and Policies for authorized officers accessing the TOE. The TOE enforces authorized officer-configurable policies on access to sensitive data:
SecureMi® Endpoint requires the end-users to key-in a correct OTP to retrieve quarantined data on targeted machines.
Data Discovery Policies enforce rules governing the suitability of files on targeted machines to store sensitive data.
SecureMi® Endpoint provides a secure vault for end-users to store sensitive data.

1.4.2 Physical Boundaries

12 The TOE includes both logical and physical boundaries, which are described in Section 2.3.1 and 2.3.2 of the Security Target (Ref [6]).

1.5 Clarification of Scope

13 The TOE is designed to be suitable for use in well-protected environments that have effective countermeasures, particularly in the areas of physical access, trained personnel, and secure communication in accordance with the user guidance supplied with the product.

14 Section 2.3 of this document describes the scope of the evaluation which was limited to those claims made in the Security Target (Ref [6]).

15 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

16 This section summarises the security aspects of the environment/configuration in which the IT product is intended to operate. Consumers should understand their own IT environments that are required for secure operation of the TOE, which is defined in the Security Target (Ref [6]).

1.6.1 Usage assumptions

17 Assumption for the TOE usage as listed in Security Target:

a) Authorized officers and users are non-hostile, appropriately trained, and follow all user guidance, installation guidance and configuration guidance. Mobile device users are not willfully negligent or hostile, and use the device within compliance of a reasonable Enterprise security policy.

1.6.2 Environment assumptions

18 Assumptions for the TOE environment listed in the Security Target are:

a) The TOE shall be located in a physically secure environment that can be accessed only by authorized personnel.

b) All hardware and third party software supporting the TOE are reliable and operating in good condition. All supporting third party software must be updated with services packs, fixes, patches and anti-virus patterns.

c) When the internal network environment changes due to change in the network configuration, host and services service increase or decrease, the changed environment and security policy shall immediately be reflected in the TOE operation policy so that security level can be maintained to be the same as before. The platforms on which the TOE operates shall be able to provide reliable time stamps.

d) IT environment will provide a secure line of communication between distributed portions of the TOE and between the TOE and remote authorized officers.

1.7 Evaluated Configuration

19 The evaluated configuration is according to the Preparative Guidance.

20 The TOE is delivered as an appliance by the developer, and the administrator must then make the following configuration charges:

a) Please ensure that the minimum system requirements described in ST are met before starting the installation.

b) The TOE must be protected against attacks on the underlying hardware, software and network.

c) All access to the administrator interfaces and the underlying OS should be restricted to trusted administrators only.

d) The administrators must be well trained and actively working to keep the product correctly configured and otherwise protected against all attacks.

1.8 Delivery Procedures

21 The delivery process as stated below:

a) A customer places an order with Evault for the SecureMi® (the TOE) product;

b) Once the order has been confirmed and paid for, the Evault team will produce a removable/optical media containing the evaluated version of the TOE and the relevant installation and guidance documentation;

c) This media device is then hand-delivered to the customer site, either by an Evault staff member or a third party;

d) The end user must sign a delivery notice/manifest confirming that they have received the TOE.

22 The end user is responsible to follow the acceptance procedures for the TOE as stated in SecureMi v1.2 Common Criteria Addendum document, which includes hash verification and assistance with the TOE installation.

1.9 Documentation

23 It is important that the TOE is used in accordance with the guidance documentation in order to ensure secure usage of the product.

24 The following documentation is provided by the developer to the end user as guidance to ensure secure delivery, installation and operation of the product:

[1]. SecureMi® Centralized Management Console v1.2 Installation Manual v6g

[2]. SecureMi® Centralized Management Console v1.2 Operation Manual v8e

[3]. SecureMi® Endpoint v1.2 Operation Manual v6a

[4]. SecureMi® Endpoint v1.2 Installation Manual v6b

[5]. SecureMi® Storage v1.2 Operation Manual v5a

[6]. SecureMi® Storage v1.2 Installation Manual v5b

[7]. SecureMi® v1.2 Data Protection List-v3f

2 Evaluation

25 The evaluation was conducted in accordance with the requirements of the Common Criteria, version 3.1 Revision 4 (Ref [2]) and the Common Methodology for IT Security Evaluation (CEM), version 3.1 Revision 4 (Ref [3]). The evaluation was conducted at Evaluation Assurance Level 2 (EAL2). The evaluation was performed conformant to the MyCC Scheme Policy (MyCC_P1) (Ref [4]) and MyCC Scheme Evaluation Facility Manual (MyCC_P3) (Ref [5]).

2.1 Evaluation Analysis Activities

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

2.1.1 Life-cycle support

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

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

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

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

31 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

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

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

34 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.

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

2.1.2 Development

36 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.

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

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

39 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.

40 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.

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

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

43 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.

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

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

46 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.

47 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.

48 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.

49 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.

50 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.

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

52 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.

53 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.

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

2.1.3 Guidance documents

55 The evaluators examined the operational user guidance to determine that it describes, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

56 The evaluators examined the operational user guidance to determine that it describes, for each user role, the secure use of the available interfaces provided by the TOE.

57 The evaluators examined the operational user guidance to determine that it describes, for each user role, the available security functionality and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

58 The evaluators examined the operational user guidance to determine that it describes, for each user role, each type of security-relevant event relative to the user functions that need to be performed, including changing the security characteristics of entities under the control of the TSF and operation following failure or operational error.

59 The evaluators examined the operational user guidance and other evaluation evidence to determine that the guidance identifies all possible modes of operation of the TOE (including, if applicable, operation following failure or operational error), their consequences and implications for maintaining secure operation.

60 The evaluators examined the operational user guidance to determine that it describes, for each user role, the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.

61 The evaluators examined the operational user guidance to determine that it is clear and it is reasonable.

2.1.4 IT Product Testing

62 Testing at EAL2 consists of assessing developer tests, performing independent functional tests, and performing penetration tests. The TOE testing was conducted by evaluators from CyberSecurity MySEF. The detailed testing activities, including configurations, procedures, test cases, expected results and actual results are documented in a separate Test Report.

2.1.4.1 Assessment of Developer Tests

63 The evaluators verified that the developer has met their testing responsibilities by examining their test plans, and reviewing their test results, 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).

64 The evaluators analysed the developer's test coverage and found them to be complete and accurate. The correspondence between the tests identified in the developer's test documentation and the interfaces in the functional specification, TOE design and security architecture description was complete.

2.1.4.2 Independent Functional Testing

65 At EAL2, 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 sample of the developer's test plan, and creating test cases that augment developer tests.

66 All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. The evaluators confirmed that the developer supplied test documentation includes test plans, expected test results and actual test results. The results of the independent functional tests that were developed and performed by the evaluators are consistent with the expected test results in the test documentation.

Test Title	Security Function	Descriptions
Identification& Authentication · TEST GROUP A – IDENTIFICATION & AUTHENTICATION · TEST GROUP B – ADMINISTRATION	FIA_UAU.2 FIA_UAU.7 FIA_UID.2 FIA_SOS.2 FDP_ACF.1 FMT_MOF.1 FMT_MSA.1 FMT_MSA.3 FMT_SMF.1 FMT_SMR.1	This test group comprises a series of test cases on TOE security functions that relates to the feature on identification and authentication in protecting the application and enforce access control for each user of the TOE.
User Data Protection · TEST GROUP B – ADMINISTRATION · TEST GROUP D – SETUP PATTERN · TEST GROUP E – GENERAL SETTING · TEST GROUP F – POLICY SETTING · TEST GROUP H – POLICY ENFORCEMENT	FDP_ACF.1 FDP_ACC.1 FIA_SOS.2 FMT_MOF.1 FMT_MSA.1 FMT_MSA.3 FMT_SMF.1 FMT_SMR.1 FMT_MTD.1 FDP_IFC.1 FDP_IFF.1	This test group comprises a series of test cases on TOE security functions that demonstrates how TOE administrators perform configuration on the rules and policies, as well as the enforcement of administrator configurable policies on sensitive data.
Security Management · TEST GROUP B – ADMINISTRATION · TEST GROUP C – TARGET · TEST GROUP D – SETUP PATTERN · TEST GROUP E – GENERAL SETTING · TEST GROUP F – POLICY SETTING · TEST GROUP G – AUDIT	FDP_ACF.1 FDP_ACC.1 FIA_SOS.2 FMT_MOF.1 FMT_MSA.1 FMT_MSA.3 FMT_SMF.1 FMT_SMR.1 FMT_MTD.1	This test group comprises a series of test cases on TOE security functions that relate to the feature on enforcing access control and privilege for each user of the TOE.
Security Audit · TEST GROUP G – AUDIT	FAU_GEN.1 FAU_SAR.1 FDP_ACC.1 FMT_MOF.1 FMT_SMF.1	This test group comprises a series of test cases on TOE security function that relates to the feature of security audit.

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

2.1.4.3 Penetration Testing

68 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.

69 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) IT hardware/software or other requirement for exploitation.

70 The penetration tests focused on:

a) Info gathering - Scanning

b) Cross Site Scripting(XSS)

c) Injection

d) Broken Authentication and Session Management

e) Failure to restrict URL Access

f) Endpoint-Normal Mode Environment

g) Endpoint-Safe Mode Environment

h) Endpoint-VM Environment

i) Endpoint-Multiuser PC Environment

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

2.1.4.4 Testing Results

72 Tests conducted for the TOE produced the expected results and demonstrated that the product behaved as specified in the Security Target and its functional specification. In addition, the documentation supplied as evidence for the EAL2 Common Criteria evaluation of the TOE was analysed to identify possible vulnerabilities.

3 Result of the Evaluation

73 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 SecureMi® v1.2 performed by CyberSecurity MySEF.

74 CyberSecurity MySEF, found that SecureMi® v1.2 upholds the claims made in the Security Target (Ref [6]) and supporting documentations, and has met the requirements of the Common Criteria (CC) assurance Level 2 (EAL2).

75 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

76 EAL2 provides assurance by a full security target and analysis of the SFRs in that Security Target, using a functional and interface specification, guidance documentation and a basic description of the architecture of the TOE, to understand the security behaviour.

77 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.

78 EAL2 also provides assurance through use of a configuration management system and evidence of secure delivery procedures.

3.2 Recommendation

79 The following recommendations are made:

a) Developer is recommended to keep on updating the TOE user guide and relevant documentation based on the latest information and feature updates of the TOE. Additionally, through new update releases, the developer is recommended to notify existing customers through any official communication platform on the latest updates, as well as, any changes made to the TOE security features. Thus, Consumers/Clients are aware on the latest updates made to the TOE.

b) Consumers/Clients are advised to seek assistance or guidance from the developer in any cases of special requirements to be configured on the TOE to ensure the security policies enforcement within organization are maintained.

c) Consumers/clients are advised to ensure that the TOE applies all the security objective for the operating environment thus vulnerability will not be exploitable in its operational environment.

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 4, September 2012.

[3] The Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012.

[4] MyCC Scheme Policy (MyCC_P1), v1d, CyberSecurity Malaysia, 26 February 2016.

[5] MyCC Scheme Evaluation Facility Manual (MyCC_P3), v1c, 26 February 2016.

[6] SecureMi® Security Target, Version 0.13, 4 July 2017

[7] Evaluation Technical Report SecureMi v.12, MySEF-3-EXE-E042-ETR-v1, 11 August 2017

A.2 Terminology

A.2.1 Acronyms

Table 2: List of Acronyms

Acronym	Expanded Term
CB	Certification Body
TSF data	Data created by and for the TOE, which might affect the operation of the TOE.
CC	Common Criteria (ISO/IEC15408)
CEM	Common Evaluation Methodology (ISO/IEC 18045)
CCRA	Common Criteria Recognition Arrangement
TSFI	TOE Security Functions Interface
SFR	Security Functional Requirement
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

Acronym	Expanded Term
API	Application Programming Interface
CC	Common Criteria
EAL	Evaluation Assurance Level
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
OS	Operating System
PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
OTP	One-time Password

A.2.2 Glossary of Terms

Table 3: 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 ---