MOSTI
KEMENTERIAN SAINS, TEKNOLOGI DAN INOVASI
MINISTRY OF SCIENCE, TECHNOLOGY AND INNOVATION

CyberSecurity MALAYSIA
An agency under MOSTI

C068 Certification Report

Enterprise Secure Key Manager (HPE ESKM)

File name: ISCB-3-RPT-C068-CR-1-v1
Version: v1
Date of document: 30 May 2016
Document classification: PUBLIC

Malaysian Common Criteria Evaluation & Certification Scheme™ MyCC

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

Securing Our Cyberspace

CyberSecurity Malaysia
(726630-U)

Best Brand Internet Security 2008 & 2009
STANDARDS MALAYSIA MS ISO/IEC 17021: 2011 ISMS 02082013 CB 02
MSC MALAYSIA Status Company

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

C068 Certification Report

Enterprise Secure Key Manager (HPE ESKM)

30 May 2016

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:	C068 Certification Report
DOCUMENT REFERENCE:	ISCB-3-RPT-C068-CR-1-v1
ISSUE:	v1
DATE:	30 May 2016

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 30 May 2016, 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	11 May 2016	All	Initial draft of certification report
v1	20 May 2016	All	Final certification report

Executive Summary

Enterprise Secure Key Manager (ESKM) from Hewlett Packard Enterprise, version 4.1 is the Target of Evaluation (TOE) for the Evaluation Assurance Level 2 Augmented with ALC_FLR.2 Evaluation.

The ESKM provides capabilities for generating, storing, serving, controlling and auditing access to data encryption keys. It enables organizations to protect and preserve access to business-critical, sensitive, data-at-rest encryption keys, both locally and remotely.

The TOE is an appliance that provides security policy and key management services to encrypting client devices and applications. After enrolment, clients (such as storage systems, application servers and databases) make requests to the TOE for creation and management of cryptographic keys and related metadata.

In its evaluated configuration, the TOE comprises two or more ESKM appliances configured as a single cluster, which provides redundancy and allows the TOE to continue to operate in a fully secure fashion in the event of a failure of a node in the cluster. Clustering also enables multiple ESKMs in a distributed environment to synchronize and replicate configuration information, which reduces administration overhead. Nodes in a cluster communicate with each other to maintain a synchronized configuration. Communications between nodes in a cluster occur over TLS.

The security functionality defined for the TOE is as follows:

a) Security Audit

b) Cryptographic Support

c) User Data Protection

d) Identification and authentication

e) Security Management

f) TSF Protection

g) TOE Access

h) Trusted Channel/ Path

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 function 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) Augmented with ALC_FLR.2. 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 BAE Systems Applied Intelligence MySEF (Malaysia Security Evaluation Facility) and completed on 5th May 2016.

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 Enterprise Secure Key Manager v4.1 meets their requirements. It is recommended that a potential user of Enterprise Secure Key Manager v4.1 refer to the Security Target (Ref [6]) and this Certification Report prior to deciding whether to purchase the product.

Table of Contents

Document Authorisation ii

Copyright Statement iii

Foreword iv

Disclaimer v

Document Change Log vi

Executive Summary vii

Table of Contents ix

Index of Tables x

1 Target of Evaluation 1

1.1 TOE Description 1

1.2 TOE Identification 3

1.3 Security Policy 4

1.4 TOE Architecture 4

1.4.1 Logical Boundaries 5

1.4.2 Physical Boundaries 6

1.5 Clarification of Scope 6

1.6 Assumptions 7

1.6.1 Usage assumptions 7

1.7 Evaluated Configuration 7

1.8 Delivery Procedures 7

1.9 Documentation 8

2 Evaluation 9

2.1 Evaluation Analysis Activities 9

2.1.1 Life-cycle support 9

2.1.2 Development 9

2.1.3 Guidance documents 10

2.1.4 IT Product Testing 10

3 Result of the Evaluation 13

3.1 Assurance Level Information 13

3.2 Recommendation 13

Annex A References 14

A.1 References 14

A.2 Terminology 14

A.2.1 Acronyms 14

A.2.2 Glossary of Terms 15

Index of Tables

Table 1: TOE identification 3

Table 2: List of Acronyms 14

Table 3: Glossary of Terms 15

1 Target of Evaluation

1.1 TOE Description

1 The TOE is an appliance that provides security policy and key management services to encrypting client devices and applications. After enrolment, clients (such as storage systems, application servers and databases) make requests to the TOE for creation and management of cryptographic keys and related metadata.

2 In its evaluated configuration, the TOE comprises two or more ESKM appliances configured as a single cluster, which provides redundancy and allows the TOE to continue to operate in a fully secure fashion in the event of a failure of a node in the cluster. Clustering also enables multiple ESKMs in a distributed environment to synchronize and replicate configuration information, which reduces administration overhead. Nodes in a cluster communicate with each other to maintain a synchronized configuration. Communications between nodes in a cluster occur over TLS.

3 The TOE supports two methods for servicing client requests—Key Management Service (KMS) and Key Management Interoperability Protocol (KMIP). Each method implements its own access control policy that determines who can perform operations on the objects within the scope of the policy—keys for KMS and managed objects for KMIP. KMIP managed objects include keys, certificates, and user-defined objects. Both the KMS and KMIP methods support TLS for client communications.

4 Administrators can configure and manage the TOE remotely via a web-based Graphical User Interface (GUI) or a Command Line Interface (CLI). The administrator uses HTTPS to access the GUI and Secure Shell (SSH) to connect to the CLI. The TOE also has a serial console port, but this is intended for use only during initial installation and configuration of the TOE. Administrators require privileges (also termed “access controls” in the TOE documentation) in order to configure a TOE feature or perform an operation. The TOE defines High Access Administrators, which are administrators with all privileges assigned (the built-in “admin” user is a High Access Administrator). A High Access Administrator can create other administrators and assign privileges to them.

5 All TOE users (administrators and clients) must be successfully identified and authenticated by the TOE before gaining access to any other TOE services. The TOE supports password and certificate-based authentication mechanisms. The TOE provides capabilities to configure minimum strength requirements (e.g., minimum length, required character sets) for passwords. The TOE can be configured to track the number of consecutive failed authentication attempts and block further authentication attempts for a configurable time period when the configured threshold has been met. The TOE will terminate interactive sessions that have been idle for a configurable period of time.

6 The TOE is able to generate audit records of security-relevant events occurring on the TOE, including startup and shutdown of the TOE, successful and unsuccessful administrator login attempts, and key management activities. It provides administrators with the ability to review audit records stored in the audit trail. The audit records are stored on the TOE appliance, where they are protected from unauthorized modification and deletion.

7 There are eight security functionalities covered under the scope of the evaluation which are:

Security Function	Description
Security Audit	The TOE maintains files that record security-relevant and other system events, including administrative actions, network activity, and cryptography requests. It also provides all administrators with the ability to review the contents of the audit trail, both at the Management Console and via the CLI. An administrator logged in to the CLI can view the contents of a specific log where the TOE has Log Storage and Rotation functionality.
Cryptographic Support	The TOE is a FIPS 140-2 validated cryptomodule (Certificate #2598).
User Data Protection	The TOE implements the User Data Protection security function to control access to cryptographic keys for ESKM Keys (created and managed using KMS) and KMIP objects (keys and other cryptographic objects created and managed using the KMIP protocol).
Identification and Authentication	The TOE distinguishes between two types of user—administrators, who configure and manage the TOE, and clients, who request key management services of the TOE using KMS (ESKM users) or KMIP (KMIP users). The Identification and Authentication security function provides the capability for the TOE to identify and authenticate both administrators and clients.
Security Management	The TOE can support two types of administrators—local and LDAP. Functionally, local and LDAP administrators have the same capabilities. The difference is that local administrators are defined locally on the TOE appliance, while LDAP administrators are defined on an LDAP server in the operational environment. The definition and use of LDAP administrators is excluded from this evaluation.

TSF Protection	The TOE comprises two or more ESKM appliances configured as a single cluster, which provides redundancy and allows the TOE to continue to operate in a fully secure fashion in the event of a failure of a node in the cluster. Clustering also enables multiple ESKMs in a distributed environment to synchronize and replicate configuration information, which reduces administration overhead. Nodes in a cluster communicate with each other to maintain a synchronized configuration.
TOE Access	An administrator can configure the TOE to terminate the KMS Server, KMIP, Management Console and CLI session types after a specified period of inactivity. The TOE also allows administrators to terminate their own interactive sessions.
Trusted Channel/ Path	The TOE supports communications via trusted channels with other trusted IT products such as Key management services and TOE backup and restore functions.

1.2 TOE Identification

8 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	C068
TOE Name	Enterprise Secure Key Manager (HPE ESKM)
TOE Version	4.1
Security Target Title	Hewlett Packard Enterprise Enterprise Secure Key Manager Security Target
Security Target Version	1.0
Security Target Date	29 April 2016
Assurance Level	Evaluation Assurance Level 2 Augmented with ALC_FLR.2

Criteria	Common Criteria for Information Technology Security Evaluation, September 2012, Version 3.1, Revision 4 (Ref [2])
Methodology	Common Criteria 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 Package conformant to EAL2 Augmented ALC_FLR.2
Sponsor and Developer	Hewlett Packard Enterprise 1160 Enterprise Way, Sunnyvale CA, 94089 USA
Evaluation Facility	BAE Systems Applied Intelligence MySEF

1.3 Security Policy

9 There are no organisational security policies that have been defined regarding the use of the TOE.

1.4 TOE Architecture

10 The TOE includes both logical and physical boundaries, which are described in Section 2.2 of the Security Target (Ref [6]).

11 The following figure 1 shows typical deployment architecture for that comprise the TOE. The TOE is represented as a two-node cluster. Note that the nodes can be collocated or installed at physically separate locations:

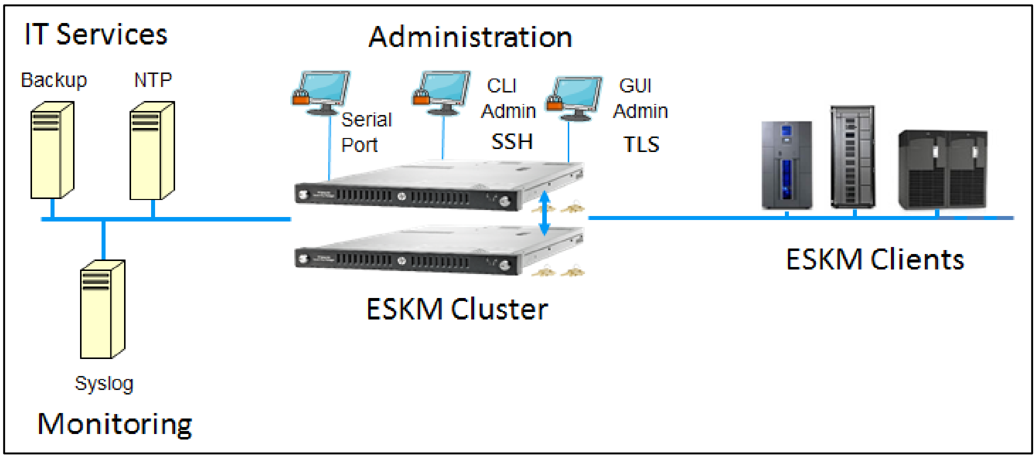

Figure 1: TOE Deployment

12 The following figure 2 shows the software architecture that comprise the TOE.

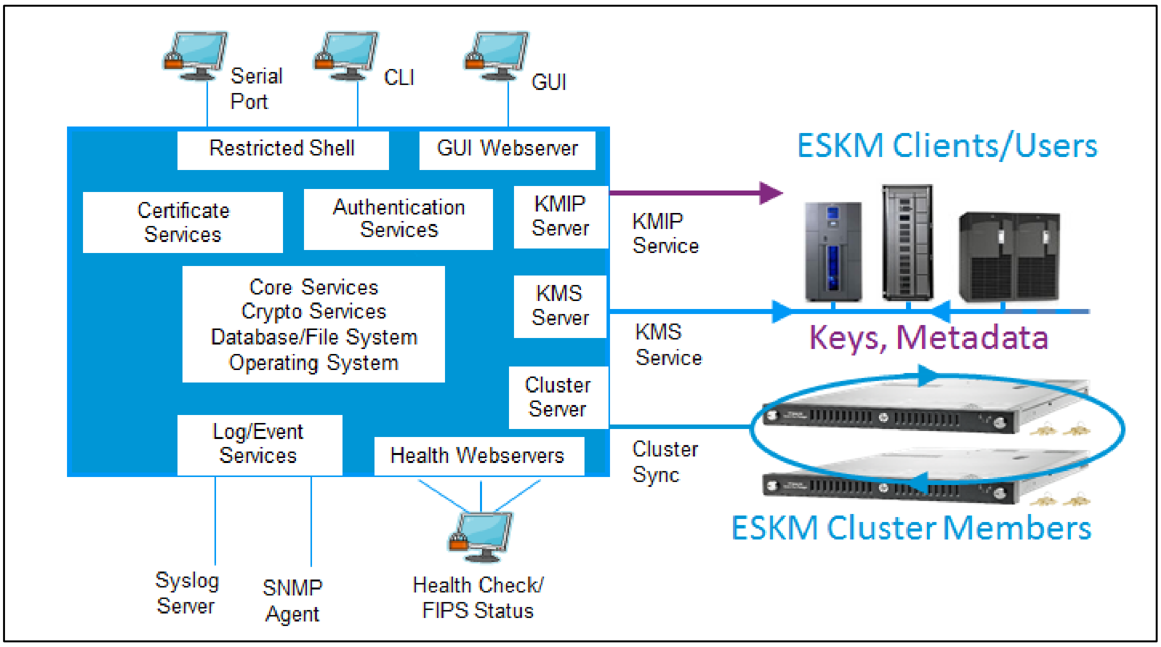

Figure 2: TOE Software Architecture

1.4.1 Logical Boundaries

13 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 TOE is able to generate audit records of security-relevant events occurring on the TOE, including startup and shutdown of the TOE, successful and unsuccessful administrator login attempts, and key management activities. It provides administrators with the ability to review audit records stored in the audit trail. The audit records are stored on the TOE appliance, where they are protected from unauthorized modification and deletion.

b) Cryptographic Support: The TOE provides the following key management services to external clients: key generation (symmetric key and asymmetric key pairs); key distribution; key storage; and key destruction. The TOE uses cryptographic protocols to protect communications: between nodes in a cluster (TLS); with external IT entities (TLS); and with remote administrators (SSH access to CLI, HTTPS access to GUI). In support of these protocols, the TOE can perform the following cryptographic operations: symmetric encryption and decryption using AES; digital signature generation and verification using RSA; cryptographic hashing using SHA-1; and keyed-hash message authentication using HMAC.

c) User Data Protection: The TOE implements an access control policy on KMS keys and a separate access control policy on KMIP objects. Access to KMS keys is based on ownership and group membership. Access to KMIP objects is based on user group membership and permissions to operate on members of object groups.

d) Identification and Authentication: The users of the TOE comprise administrators, who manage the TOE and its configuration, and clients, who request key management services from the TOE. Clients are classified as ESKM clients or KMIP clients, depending on the protocol used to access the TOE—ESKM XML for ESKM clients and KMIP for KMIP clients. The TOE identifies and authenticates all users of the TOE before granting them access to the TOE. The TOE associates a user identity and authentication data (password and/or certificate) with each client and user identity, password and privileges (or “access controls”) with each administrator. The TOE enforces minimum requirements for the construction of user passwords and provides a mechanism to lock a user account after a configured number of consecutive failed attempts to logon.

e) Security Management: The TOE implements a privilege-based security management model. Administrators are granted privileges to perform security management functions on the TOE. Each privilege grants access to a specific subset of the security management capabilities of the TOE. An administrator with all privileges is termed a High Access Administrator and is able to perform all security management functions, including creating and managing other administrator accounts and changing user and administrator passwords.

f) TSF Protection: In its evaluated configuration, the TOE comprises two or more ESKM appliances configured as a single cluster, which provides redundancy and allows the TOE to continue to operate in a fully secure fashion in the event of a failure of a node in the cluster. Communications between nodes in a cluster occur over TLS, which provides confidentiality and detection of modification of transmitted data. The TOE includes its own time source for providing reliable time stamps that are used in audit records.

g) TOE Access: The TOE will terminate interactive sessions after a period of inactivity configurable by an administrator. The TOE allows administrators to terminate their own interactive sessions.

h) Trusted Channel/ Path: The TOE provides a trusted path for TOE administrators to communicate with the TOE. The trusted path is implemented using HTTPS for access to the GUI and SSHv2 for access to the CLI. Administrators initiate the trusted path by establishing an HTTPS connection (using a supported web browser) or SSH session (using an SSH client). The trusted path is used for initial authentication and all subsequent administrative actions. The use of HTTPS or SSHv2 ensures all communication over the trusted path is protected from disclosure and undetected modification.

1.4.2 Physical Boundaries

14 The TOE includes both logical and physical boundaries, which are described in Section 2.2.3 of the Security Target (Ref [6]).

1.5 Clarification of Scope

15 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 user guidance that is supplied with the product.

16 Section 1.4 of this document described the scope of the evaluation which was limited to those claims made in the Security Target (Ref [6]).

17 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

18 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

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

a) There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.

b) The authorized administrators are not careless, wilfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

1.6.2 Environment assumptions

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

a) The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.

1.7 Evaluated Configuration

21 The evaluated configuration is described in details (see Figure 1 Deployment Architecture) as described in Section 2.2.1 of the Security Target (Ref [6]).

1.8 Delivery Procedures

22 The delivery process for the TOE consists of:

a) Product Orders: When Hewlett Packard Enterprise receives an order for a product, they notify the HPE supply chain department to assemble the product and ship it to the customer to fulfil the order.

b) Order Tracking: Each product shipped by the HPE supply chain department is uniquely identified by its order number. The HPE Supply chain department makes this information available to Hewlett Packard Enterprise should a problem arise.

c) Order Shipment: The HPE supply chain department packages the Hewlett Packard Enterprise products in boxes for shipment. Shipments include the requested hardware and embedded software, while update software/software patches, and configuration guide documents are downloaded from the Hewlett Packard Enterprise website (https://softwaresupport.hp.com).

d) Order Security: The HPE Supply chain department is a commercial organization providing assembly and packaging services for Hewlett Packard Enterprise.

Additionally, since the packages have labels affixed to them, it would be evident to customers if tampering occurred if the labels were replaced; thus, the security of the product is ensured. This section is of particular importance, as it provides a baseline for the evaluated product delivery procedures.

1.9 Documentation

23 It is important that the TOE is used in accordance with 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]. HP Enterprise Secure Key Manager 4.1 User Guide, C8Z61-9000C, December 2014

[2]. HP Enterprise Secure Key Manager 4.1 Installation and Replacement Guide, C8Z61-9001C, December 2014

[3]. HP Enterprise Secure Key Manager 4.1 Software Version 6.1.0 Release Notes, C8Z61-9002C, December 2014

[4]. HP Enterprise Secure Key Manager Key Protection Best Practices, 4AA2-1403ENW, rev. 4, March 2011.

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+) Augmented ALC_FLR.2. 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 An analysis of the TOE configuration management system and associated documentation was performed. The evaluators confirmed that the TOE provided for evaluation is labelled with its reference and labels are consistent.

28 The evaluators examined the method of identifying items, how configuration items are uniquely identified, and the items list are identified consistent with the Configuration Management (CM) documentation.

29 The evaluators examined, confirmed and checked that CM is included, items identified in the configuration list are being maintained by the CM system, the CM system records identified by the CM plan, and the CM system is being operated in accordance with the CM plan.

2.1.2 Development

30 The evaluators examined the security architecture description that it contains sufficient information to demonstrate that the TSF is able to protect itself from tampering by untrusted active entities. The security architecture description presents an analysis that adequately describes how the SFR-enforcing mechanisms cannot be bypassed.

31 The evaluators analysed 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).

32 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 behaviour of the SFR-enforcing subsystems.

33 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.

2.1.3 Guidance documents

34 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.

2.1.4 IT Product Testing

35 Testing at EAL2+ Augmented ALC_FLR.2 consists of assessing developer tests, performing independent functional test, and performing penetration tests. The TOE testing was conducted by evaluators from BAE Systems Applied Intelligence MySEF. The detailed testing activities, including configurations, procedures, test cases, expected results and actual results are documented in a separate Test Plan Reports.

2.1.4.1 Assessment of Developer Tests

36 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).

37 The evaluators analysed the developer's test coverage and found it 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

38 At EAL2+ Augmented ALC_FLR.2, independent functional testing is the evaluation conducted by evaluator 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 augmented developer tests.

39 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 as developed and performed by the evaluators are consistent with the expected test results in the test documentation.

Identifier	Security Function	Descriptions
F001	FIA_ATD.1, FIA_SOS.1, FMT_MTD.1(1), FMT_MTD.1(2), FMT_MTD.(6), FMT_SMF.1.1, FMT_REV.1,	This test aims to verify that the TOE performs: Identification and authentication, Security Management functions and TOE Access functions

Identifier	Security Function	Descriptions
	FTA_SSL.4, FIA_UAU.5	
F002	FIA_UID.2.1, FMT_MTD.1.1(1), FMT_MTD.1.1(2), FMT_MTD.1.1(3), FMT_MTD.1.1(4), FMT_MTD.1.1(5), FMT_MTD.1.1(7), FMT_SMR.1.1, FMT_SMR.1.2, FIA_AFL.1.1, FIA_AFL.1.2, FMT_SMF.1.1, FTP_TRP.1.1, FTP_TRP.1.2, FTP_TRP.1.3, FCS_COP.1(1), FCS_COP.1(2), FCS_COP.1(3), FCS_COP.1(4), FIA_UAU.5	This test aims to verify that the TOE performs Identification and authentication, Security Management functions, Trusted Channels/ Path and Cryptographic Support functions
F003	FTA_SSL.3, FPT_FLS.1, FPT_ITT.1, FPT_ITT.3.1, FPT_ITT.3.2, FIA_UAU.2.1, FIA_UAU.5	This test aims to verify that the TOE performs: Identification and authentication, Protection of the TSF and TOE Access functions
F004	FDP_ACC.1.1(1), FDP_ACC.1.1(2), FDP_ACF.1.1(1), FDP_ACF.1.2(1), FDP_ACF.1.2(2), FMT_MSA.1.1(1), FMT_MSA.1.1(2), FMT_MSA.3.1(1), FMT_MSA.3.2(1), FMT_MSA.3.1(2), FMT_MSA.3.2(2), FIA_UID.2, FIA_UAU.5, FCS_CKM.1, FCS_CKM.2, FCS_CKM.3, FCS_CKM.4	This test aims to verify that the TOE performs User Data Protection, Security Management, Identification and Authentication, and Cryptographic Support functions
F005	FMT_MOF.1(2), FMT_MOF.1(3), FMT_MOF.1(4), FMT_MOF.1(5), FMT_SMF.1.1, FIA_UAU.5	This test aims to verify that the TOE performs Security Management functions and Identification and Authentication functions
F006	FAU_SAR.1.1, FAU_SAR.1.2, FAU_GEN.1.1, FAU_GEN.1.2,	This test aims to verify that the TOE performs Security Audit functions, Security Management, Trusted Channels/ Path,

Identifier	Security Function	Descriptions
	FAU_GEN.2.1, FAU_STG.1.1, FAU_STG.1.2, FMT_MOF.1.1(1), FTP_ITC.1, FIA_UAU.5, FCS_CKM.1, FCS_CKM.2, FCS_CKM.3, FCS_CKM.4	Identification and Authentication, and Cryptographic Support functions

2.1.4.3 Penetration Testing

40 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.

41 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 (specialist 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.

42 The penetration tests focused on the following vulnerability:

a) Open ports

b) Common vulnerabilities on running server

c) Common web vulnerabilities

d) Weak Cipher

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

2.1.4.4 Testing Results

44 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. In addition, the documentation supplied as evidence for the EAL2+ ALC_FLR.1 Common Criteria evaluation of the TOE was analysed to identify possible vulnerabilities.

3 Result of the Evaluation

45 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 Enterprise Secure Key Manager performed by BAE Systems Applied Intelligence MySEF.

46 BAE Systems Applied Intelligence MySEF, found that Enterprise Secure Key Manager 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 Augmented with ALC_FLR.2 (EAL2+ALC_FLR.2).

47 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

48 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.

49 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.

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

3.2 Recommendation

51 The following recommendations are made:

a) Potential purchasers of the TOE should review the intended operational environment and ensure that they are comfortable that the stated security objectives for the operational environment can be suitably addressed.

b) The developers should make themselves familiar with the developer guidance provided with the TOE and pay attention to all security warnings.

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] Hewlett Packard Enterprise Enterprise Secure Key Manager Security Target, Version 1.0, 29 April 2016.

[7] Evaluation Technical Report, HPE Enterprise Secure Key Manager, EAU000257-S029-ETR, Version 1.0, 10 May 2016.

A.2 Terminology

A.2.1 Acronyms

Table 2: 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 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
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.

Term	Definition and Source
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 ---