M006 Maintenance Report

File name: ISCB-5-RPT-M006-AMR-v1
Version: v1
Date of document: 3 March 2017
Document classification: PUBLIC

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

CyberSecurity Malaysia
(726630-U)
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

M006 Maintenance Report

Enterprise Secure Key Manager v5.0

3 March 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:	M006 Maintenance Report
DOCUMENT REFERENCE:	ISCB-5-RPT-M006-AMR-v1
ISSUE:	v1
DATE:	3 March 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

Document Change Log

RELEASE	DATE	PAGES AFFECTED	REMARKS/CHANGE REFERENCE
d1	1/3/2017	All	Initial draft of maintenance report
v1	3/3/2017	All	Final version of maintenance report

Table of Contents

Document Authorisation ii

Copyright Statement iii

Document Change Log iv

Table of Contents v

1 Introduction 1

2 Description of Changes 3

2.1. Changes to the product associated with the certified TOE 3

4 Affected Developer Evidence 6

Annex A References 7

Result of the Analysis 8

1 Introduction

1 Enterprise Secure Key Manager (ESKM), version 5.0, from Hewlett Packard Enterprise. 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.

2 The purpose of this document is to enable developers to provide assured products to the IT consumer community in a timely and efficient manner against the certified and updated version of TOE as in table 1 identification below.

3 Identification Information

Table 1 – Identification Information

Assurance Maintenance Identifier	M006
Project Identifier	C068
Evaluation Scheme	Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme
Impact Analysis report	Impact Analysis Report – Enterprise Secure Key Manager v5.0
New TOE	Enterprise Secure Key Manager v5.0
Certified TOE	Enterprise Secure Key Manager v4.1
New Security target	Hewlett Packard Enterprise Enterprise Secure Key Manager Security Target v1.0, 10 March 2017
Certified Security Target	Enterprise Secure Key Manager Security Target v1.0, 29 April 2016
Evaluation Level	EAL2 + ALC_FLR.2
Evaluation Technical Report (ETR)	EAU000257-S029-ETR v1.0, 10 May 2016
Criteria	Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Components, September 2012, Version 3.1, Revision 4 Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Components, September 2012, Version 3.1 Revision 4
Methodology	Common Evaluation Methodology for Information Technology Security Evaluation, September 2012, Version 3.1 Revision 4 (Ref[VIII])
Common Criteria Conformance	CC Part 2 Conformant CC Part 3 Conformant

	Package conformant to EAL2 Augmented (ALC_FLR.2)
Protection Profile Conformance	None
Sponsor & Developer	Leidos Inc. 6841 Benjamin Franklin Drive Columbia, MD 21046
Evaluation Facility	BAE Systems Applied Intelligence - MySEF

2 Description of Changes

3 Hewlett Packard Enterprise (HPE) has issued a new release of the Enterprise Secure Key Manager (ESKM) version 5.0. There were a series of minor updates to the ESKM since its certification version 4.1 in May 2016.

2.1. Changes to the product associated with the certified TOE

4 The following features have been added in Enterprise Secure Key Manager v4.1 (ref[I]):

ESKM 4.1 Software version 6.2.0

i. Public key authentication for CLI administration sessions has been added. A public key can be associated with an ESKM Administrator. This public key can then be used to authenticate the administrator when they log in to the ESKM server via an SSH version 2 session. Public keys can be added, deleted, or viewed using the CLI or the Management Console.

ii. Support for IPv6 addresses has been added. Both the management console and the CLI can be accessed by clients using IPv6 address. The KMS and KMIP servers can be accessed by clients using IPv6 addresses. Clients using IPv6 addresses can obtain health check information for both the KMS and KMIP servers. In addition, the following ESKM features, which use SCP to move files, support IPv6 addresses: backup, restore, scheduled backup, transfer/rotate logs, certificate import, and software upgrade/install. Both the source and target host systems must be in the same local IPv6 network.

iii. Support for KMIP 1.3.

iv. Ability to specify a server certificate for web administration has been added.

v. TLS 1.0, TLS 1.1, and TLS 1.2 protocol versions are individually selectable for the KMS and KMIP servers.

vi. KMIP server supports the ability to configure how clients are authenticated.

vii. KMIP server supports CMAC mode authentication for 3DES and AES operations.

viii. KMIP server supports ECDSA-256 and ECDSA-384 X.509 certificates to support Suite B Cryptography. The ESKM server cannot create an EC local CA certificate, nor can it sign EC certificate requests. EC certificates must be signed externally and the imported into the ESKM system.

ESKM 4.1 Software version 6.2.1

i. Weak ciphers for the KMS SSL/TLS connections removed.

ii. CLI command “no export cipherspec” removed.

iii. Upgraded to 1.0.1t Open SSL Library

iv. The KMS server supports AES-128-SHA-256, AES-256-SHA-256, and AES-128-GCM-SHA-256 cipher suites for TLS 1.2.

EKSM 4.1 Software version 6.2.2

i. OpenSSH upgraded.

ii. OpenSSL upgraded.

iii. Added following elements to the<UserModifyRequest> XML commands:

- <KMIPObjectGroup>, which allows the user (with administrator permissions> to change the object group into which the user's objects belong.
- <CertificateData>, which allows the user (with administrator permissions) to add, change, or renew the user's certificate.

ESKM 5.0 Software version 7.0.0

i. This release of the ESKM consists of the following generic updates and the features specified in ESKM 4.1 Software version 6.2.0:

ii. Rebranding of the ESKM appliance and management console as a Hewlett Packard Enterprise product offering.

iii. Support for next generation (GEN9) appliance platform with a full hardware refresh.

iv. SHA-256 updates for compliance with current security standards and best practices.

v. Enhanced system health status reporting.

ESKM 5.0 Software version 7.0.1

i. Weak ciphers for the KMS SSL/TLS connections removed.

ii. CLI command "no export cipherspec" removed.

iii. Upgraded to 1.0.1t Open SSL Library.

iv. The KMS server supports AES-128-SHA-256, AES-256-SHA-256, and AES-128-GCM-SHA-256 cipher suites for TLS 1.2.

ESKM 5.0 Software version 7.0.2

i. Open SSH upgraded.

ii. OpenSSL upgraded.

iii. Added following elements to the<UserModifyRequest> XML commands:

- <KMIPObjectGroup>, which allows the user (with administrator permissions> to change the object group into which the user's objects belong.
- <CertificateData>, which allows the user (with administrator permissions) to add, change, or renew the user's certificate

5 The following items provide clarification or describe issues fixed in this release (ref[I]):

i. Replication failure after changing the local Certificate Authority (CA) name.

ii. Revoked server certificate can be selected.

iii. Public key size restriction for administrator authentication.

iv. Trusted CA List Profile for KMIP Server Authentication Settings is not replicated.

v. Certificate information is not returned.

vi. KMS restarts.

vii. No SNMP trap sent after multiple failed administrative login attempts.

viii. Replication failure in a networked cluster.

ix. User configuration change is not replicated when the ESKM server is under heavy load.

x. Unable to start KMIP server after restoring a backup.

xi. Multiple KMIP server restart events.

xii. Management console windows do not display correctly.

xiii. Public key authentication does not support all key sizes.

6 There are no significant changes to secure delivery and distribution site, configuration management procedures, site security procedures and configuration management tools used to develop the TOE (ref[II]).

4 Affected Developer Evidence

7 The affected developer evidence submitted associated for the assurance continuity required by the CCRA Assurance Continuity: CCRA Requirements Version 2.1 (2012-06-01) June 2012 are:

a) Enterprise Secure Key Manager Security target, Version 0.2

b) HP Enterprise Secure Key Manager 4.2 Software Version 6.2.0 Release Notes

c) HP Enterprise Secure Key Manager 4.2 Software Version 6.2.1 Release Notes

d) HP Enterprise Secure Key Manager 4.2 Software Version 6.2.2 Release Notes

e) Enterprise Secure Key Manager 5.0 Software Version 7.0.0 Release Notes

f) Enterprise Secure Key Manager (ESKM) v5 – Software version 7.0.0 Release Notes

g) Enterprise Secure Key Manager v5 Software Version 7.0.1 Release Notes

Annex A References

[I] Impact Analysis Report (IAR), EAU000426.05-IAR1.0, 27 FEBRUARY 2017, version 5.0

[II] Enterprise Secure Key Manager Security Target Version, v5.0, 25 JANUARY 2017

[III] Hewlett Packard Enterprise Secure Key Manager Security Target, Version 1.0, 29 APRIL 2016

[IV] Assurance Continuity: CCRA Requirements Version 2.1 (2012-06-01) June 2012

[V] Declaration of Similarity (DoS) for Product Families, autxa_1002_DoS_05, 2 March 2015

[VI] Arrangement on the recognition of Common Criteria Certificates in the field of Information Technology Security, May 2000.

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

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

[IX] MyCC Scheme Policy (MyCC_P1), v1a, CyberSecurity Malaysia, December 2009.

[X] MyCC Scheme Evaluation Facility Manual (MyCC_P3), v1, December 2009.

[XI] C068 Evaluation Technical Report for HPE Enterprise Secure Key Manager, EAU000257-S029-ETR, Version 1.0, 10 May 2016

Result of the Analysis

8 The outcome of the review found that none of the modifications significantly affects the security mechanisms that implement the functional requirements of the Security Target (ref[II]) as required in accordance of Assurance Continuity: CCRA Requirements Version 2.1 (2012-06-01) June 2012 (ref[IV]).

9 The nature of the changes leads to the conclusion that they are classified as minor changes. Therefore, it is agreed based on the evidences given that the assurance is maintained for this version of the product.

--- END OF DOCUMENT ---