M009 Maintenance Report

File name: ISCB-5-RPT-M009-AMR-v1
Version: v1
Date of document: 08 March 2019
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

Securing Our Cyberspace

M009 Maintenance Report

Utimaco Enterprise Secure Key Manager, version 5.1

08 March 2019

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:	M009 Maintenance Report
DOCUMENT REFERENCE:	ISCB-5-RPT-M009-AMR-v1
ISSUE:	v1
DATE:	08 March 2019

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	6/3/2019	All	Initial draft of maintenance report
v1	7/3/2019	All	Final version of maintenance report

Table of Contents

1 Introduction

1 The Enterprise Secure Key Manager (ESKM), version 5.1 provides capabilities for generating, storing, serving, controlling and auditing access to data encryption keys. It enables organisations 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 the TOE as identified in table 1 below.

3 Identification Information:

Table 1 – *Identification Information*

Assurance Maintenance Identifier	M009
Project Identifier	C068
Evaluation Scheme	Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme
Impact Analysis report	Impact Analysis Report, Utimaco Enterprise Secure Key Manager (ESKM) v5.1, GOXX2247-IAR, 22 Feb 2019, version 1.0
New TOE	Utimaco Enterprise Secure Key Manager, version 5.1
Certified TOE	Enterprise Secure Key Manager, version 5.0
New Security target	Utimaco Enterprise Secure Key Manager Security Target v1.0, 19 February 2019
Certified Security Target	Hewlett Packard Enterprise Enterprise Secure Key Manager Security Target v1.0, 10 March 2017
Evaluation Level	Evaluation Assurance Level 2 (EAL2) Augmented with ALC_FLR.2
Evaluation Technical Report (ETR)	EAU000257-S029-ETR v1.0, 10 May 2016
Criteria	Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1, Revision 5, April 2017 Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Components, Version 3.1, Revision 5, April 2017 Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Components, Version 3.1, Revision 5, April 2017

Methodology	Common Evaluation Methodology for Information Technology Security Evaluation, September 2012, Version 3.1 Revision 5, April 2017
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	Utimaco Inc. 900 E Hamilton Ave., Suite 400 Campbell, CA 95008 USA
Evaluation Facility	BAE Systems Applied Intelligence - MySEF

2 Description of Changes

4 Utimaco has acquired the Atalla product line previously owned by Micro Focus (and before that, Hewlett Packard Enterprise (HPE)) and issued a new release of the previously certified Enterprise Secure Key Manager 5.0. The changes to the TOE consist of thirty-eight (38) product enhancements/additions - no additional security functionality was added, and no existing security functionality was removed (ref[II]).

2.1. Changes to the product associated with the certified TOE

5 The following features and enhancement have been added in Enterprise Secure Key Manager, version 5.1 (ref[II]):

Table 2 - *Enterprise Secure Key Manager enhancements/additions*

Change	Description
Weak cipher suites removed	Removed weak ciphers for the KMS SSL/TLS connections
CLI command removed	Removed the “no export cipherspec” CLI command
Supported cipher suites	The KMS server now supports the following cipher suites for TLS 1.2: • AES-128-SHA-256 • AES-256-SHA-256 • AES-128-GCM-SHA-256
XML command update	Added the following elements to the <UserModifyRequest> XML command: • <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
Certificate Authorities (CAs) expiration date	Extended the expiration date of imported known Certificate Authorities (CAs) to the year 2049
KMIP support	Added support for KMIP version 1.4
IPv6 default gateway support for CLI	Added and modified CLI commands to support an IPv6 default gateway
IPv6 default gateway configuration for management console	Added the ability to specify an IPv6 default gateway from the management console
Weak SSH algorithms removed	Removed support for weak SSH algorithms and added support for stronger SSH algorithms.
SNMP trap alerts	SNMP trap is sent after five consecutive incorrect admin login attempts (if SNMP is enabled)
List of local CA certs	<CertificateInfoRequest> returns the completed list of Local CA certs, even if there is a certificate with status Request Pending

Change	Description
Replication of Local CA name change	Local CA name change is successfully replicated to other cluster nodes
Company rebranding	Micro Focus rebranding
Cluster performance	Improved cluster performance
Backup options	Selective backup option for KMIP objects
HDD failure reporting	Enhanced HDD failure reporting
Supported cipher suites	Support stronger KMS cipher suites (already supported via KMIP) • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • RSA-RSA-AES256-GCM-SHA384
Support for TLS 1.2	Use TLS 1.2 for cluster communication
SSH configuration options	Provide SSH algorithm configuration options
SSH maximum login attempts	Support for SSH admin maximum login attempts
Certification creation	Support 3072-bit certificate creation via GUI (already supported via KMIP and cert import)
KMIP 1.4 support	Added support for KMIP 1.4 mandatory attributes (Sensitive, Always Sensitive, Extractable, Never Extractable)
Fixed vulnerabilities and bugs in v5.0.6	Fixed vulnerabilities and bugs, including • KMS server memory leak • Key Query by Creation Date • Help page searching
ESKM key query download	Download option for ESKM key query (key names)
Company rebranding	Rebranded Management Information Base (MIB) to Micro Focus
Fixed bugs in v5.0.8	Fixed bugs, including • Sorting ESKM by Creation Date • ESKM and KMIP group queries • Replication improvements
TLS support	TLS configuration support for LDAP
LDAP support	LDAP support in FIPS mode
Supported algorithms	Support stronger algorithms for ESKM backup (AES instead of 3-key TDES)
KMIP 2.0 support	Initial KMIP 2.0 support
ECDSA support	Support for ECDSA key pair generation via KMIP
ECDHE support	ECDHE key agreement support for cluster communication
Performance enhancements	Performance improvement in user and key creation
CentOS Linux update	Update to CentOS Linux release 7.4.1708
OpenSSL update	Update to OpenSSL 1.0.2p

Change	Description
OpenSSH update	Update to OpenSSH 7.7p1
Expired CAs	Removed expired known CAs
Fixed vulnerabilities and bugs in v5.1	Fixed vulnerabilities and defects, including • KMS restart and health check failure • L1 Terminal Fault Vulnerability • Meltdown and Spectra Vulnerabilities • Privilege escalation Vulnerability • OpenSSH Username enumeration Vulnerability • DCCP double free Vulnerability

6 The following items provide description of changes and the impact to this TOE release (ref[II]):

Table 3 – *Description of changes and impact*

Identifier	Description of changes	Impact
Enterprise Secure Key Manager, version 5.1	LDAP support in FIPS mode	Minor
	Initial KMIP 2.0 support	Minor
	Support for ECDSA key pair generation via KMIP	Minor
	ECDHE key agreement support for cluster communication	Minor
	Support stronger algorithms for ESKM backup (AES instead of 3-key TDES)	Minor
	Performance improvement in user and key creation	Minor
	Removed expired known CAs	Minor
	Update to CentOS Linux release 7.4.1708	Minor
	Update to OpenSSL 1.0.2p	Minor
	Update to OpenSSH 7.7p1	Minor
	Fixed vulnerabilities and defects, including • KMS restart and health check failure • L1 Terminal Fault Vulnerability • Meltdown and Spectra Vulnerabilities • Privilege escalation Vulnerability • OpenSSH Username enumeration Vulnerability • DCCP double free Vulnerability	Minor

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

3 Affected Developer Evidence

8 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) Utimaco Enterprise Secure Key Manager Security Target, version 1.0, 19 February 2019

b) Enterprise Secure Key Manager v5.1, Software Version 7.1.0, User's Guide, October 2018

c) Enterprise Secure Key Manager v5.1, Installation and Replacement Guide, October 2018

d) Utimaco Enterprise Secure Key Manager (ESKM) Life Cycle Document, Version 1.0, 6 December 2018

4 Result of the Analysis

9 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[IV]) as required in accordance of Assurance Continuity: CCRA Requirements Version 2.1 (2012-06-01) June 2012 (ref[V]).

10 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.

Annex A References

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

[II] Impact Impact Analysis Report (IAR), GOXX2247-IAR 1.0, 22 FEBRUARY 2019, version 1.0

[III] Hewlett Packard Enterprise Enterprise Secure Key Manager Security Target v1.0, 10 March 2017

[IV] Utimaco Enterprise Secure Key Manager Security Target Version 1.0, 19 February 2019

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

[VI] Arrangement on the recognition of Common Criteria Certificates in the field of Information Technology Security, 2 July 2014.

[VII] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1, Revision 5, April 2017

[VIII] Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Components, Version 3.1, Revision 5, April 2017

[IX] Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Components, Version 3.1, Revision 5, April 2017

[X] Common Evaluation Methodology for Information Technology Security Evaluation, September 2012, Version 3.1 Revision 5, April 2017

[XI] ISCB Product Certification Scheme Policy v1a, 19 June 2017

[XII] ISCB Evaluation Facility Manual (ISCB_EFM), v1, 22 June 2018.

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

--- END OF DOCUMENT ---