Enterprise Secure Key Manager

FIPS 140-2
Security Policy

Level 2 Validation

Document Version 1.1
May 7, 2013

On November 5, 2018, the Atalla business was acquired by Utimaco Inc. For aspects of this Security Policy document, the rest of this document will refer to the HP Enterprise Secure Key Manager. However, the Vendor is now Utimaco Inc.

Table of Contents

Table of Figures

Table of Tables

1 Introduction

1.1 Purpose

This document is a non-proprietary Cryptographic Module Security Policy for the HP Enterprise Secure Key Manager (ESKM) from Hewlett-Packard Company. Federal Information Processing Standards (FIPS) 140-2, *Security Requirements for Cryptographic Modules*, specifies the U.S. and Canadian Governments' requirements for cryptographic modules. The following pages describe how HP's ESKM meets these requirements and how to use the ESKM in a mode of operation compliant with FIPS 140-2. This policy was prepared as part of the Level 2 FIPS 140-2 validation of the HP ESKM 3.0 (Hardware P/N AJ585A, Version 3.0; Firmware Version: 5.0.0) and ESKM 3.1 (Hardware P/N C8Z51AA, Version 3.1; Firmware Version: 5.1.0).

More information about FIPS 140-2 and the Cryptographic Module Validation Program (CMVP) is available at the website of the National Institute of Standards and Technology (NIST): http://csrc.nist.gov/groups/STM/cmvp/index.html.

In this document, the HP Enterprise Secure Key Manager is referred to as the *ESKM*, the *module*, or the *device*.

1.2 References

This document deals only with the operations and capabilities of the module in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the module from the following sources:

- The HP website (http://www.hp.com) contains information on the full line of products from HP.
- The CMVP website (http://csrc.nist.gov/groups/STM/cmvp/index.html) contains contact information for answers to technical or sales-related questions for the module.

2 HP Enterprise Secure Key Manager

2.1 Overview

HP provides a range of security products for banking, the Internet, and enterprise security applications. These products use encryption technology—often embedded in hardware—to safeguard sensitive data, such as financial transactions over private and public networks and to offload security processing from the server.

The HP Enterprise Secure Key Manager is a hardened server that provides security policy and key management services to encrypting client devices and applications. After enrollment, clients, such as storage systems, application servers and databases, make requests to the ESKM for creation and management of cryptographic keys and related metadata.

Client applications can access the ESKM via its Key Management Service (KMS) server. Configuration and management can be performed via web administration, Secure Shell (SSH), or serial console. Status-monitoring interfaces include a dedicated FIPS status interface, a health check interface, and Simple Network Management Protocol (SNMP).

The deployment architecture of the HP Enterprise Secure Key Manager is shown in Figure 1 below.

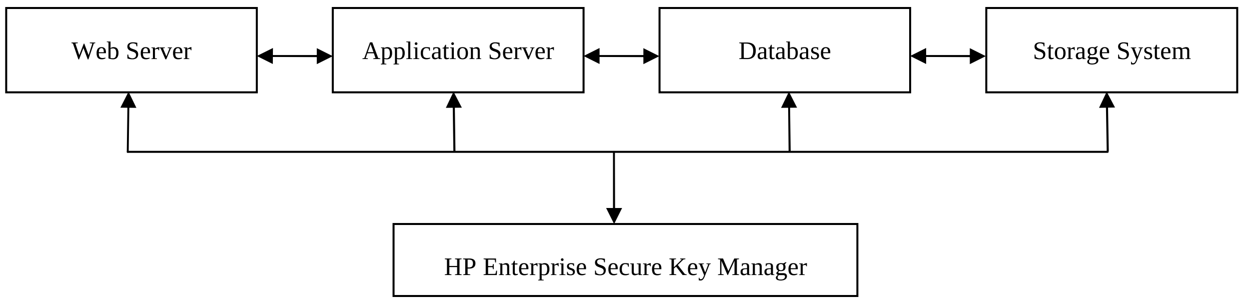

Figure 1 – Deployment Architecture of the HP Enterprise Secure Key Manager

2.2 Cryptographic Module Specification

The HP Enterprise Secure Key Manager is validated at FIPS 140-2 section levels shown in Table 1.

Table 1 – Security Level per FIPS 140-2 Section

Section	Section Title	Level
1	Cryptographic Module Specification	3
2	Cryptographic Module Ports and Interfaces	2
3	Roles, Services, and Authentication	3
4	Finite State Model	2
5	Physical Security	2
6	Operational Environment	N/A
7	Cryptographic Key Management	2
8	EMI/EMC	2

Section	Section Title	Level
9	Self-Tests	2
10	Design Assurance	2
11	Mitigation of Other Attacks	N/A

The block diagram of the module is given in Figure 2. The cryptographic boundary is clearly shown in the figure. Notice that the power supplies are not included in the boundary.

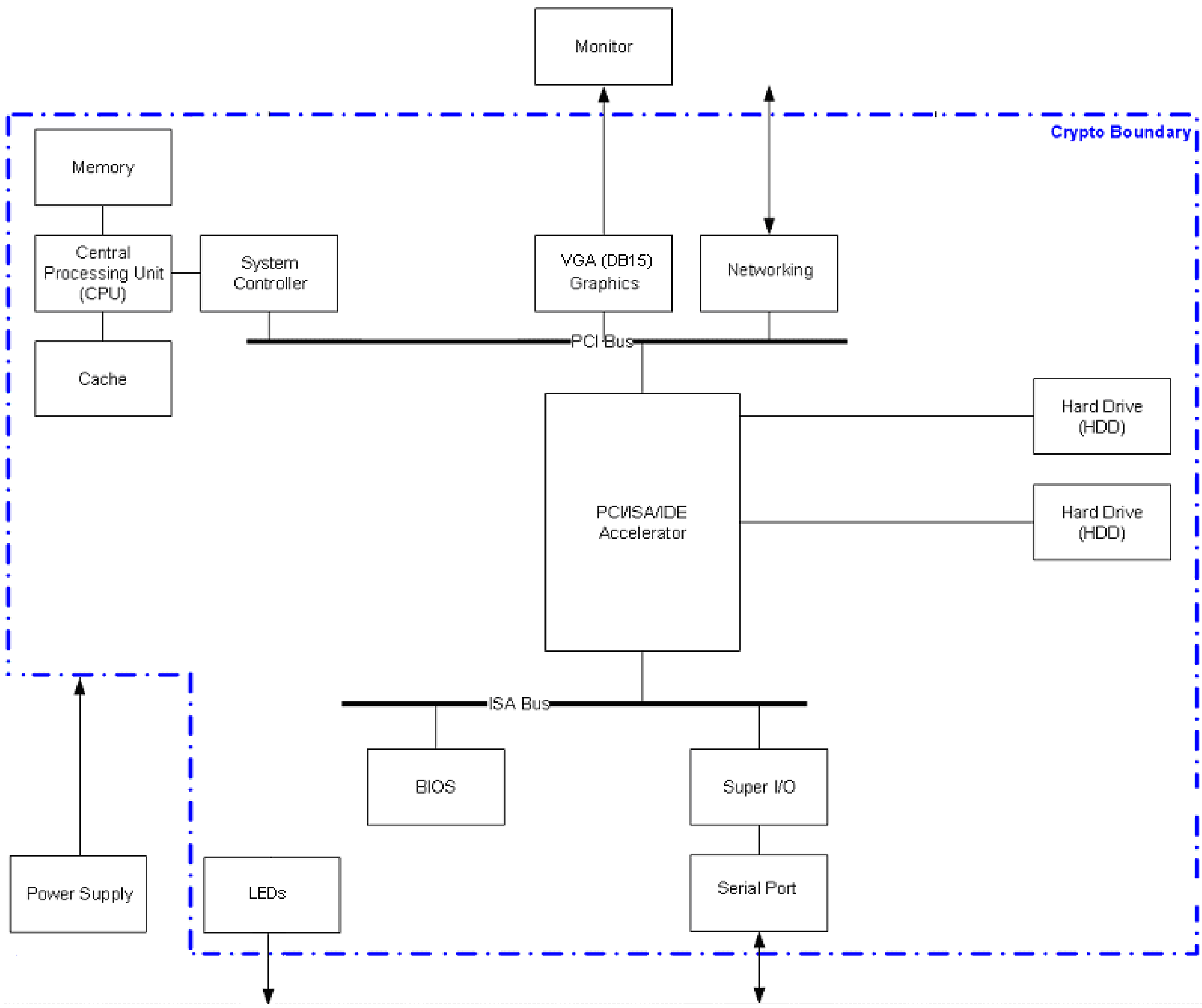

Figure 2 – Block Diagram of ESKM

In the FIPS mode of operation, the module implements the following Approved algorithms:

- Advanced Encryption Standard (AES) encryption and decryption: 128, 192, and 256 bits, in Electronic Codebook (ECB) and Cipher Block Chaining (CBC) modes (Certificate #2069)
- Triple Data Encryption Standard (Triple-DES or TDES) encryption and decryption: 168 bits (3-key), in ECB and CBC modes (Certificate #1328)
- Secure Hash Algorithm (SHA)-1, SHA-256, SHA-384, SHA-512 (Certificate #1802)

- Keyed-Hash Message Authentication Code (HMAC)-SHA-1 and HMAC-SHA-256 (Certificate #1254)
- Rivest, Shamir, and Adleman (RSA) American National Standard Institute (ANSI) X9.31 key generation, signature generation, and signature verification: 1024 (signature verification only) and 2048 bits (Certificate #1073)
- Deterministic Random Bit Generator (DRBG) using AES in CTR mode (Certificate #207)
- Diffie-Hellman key agreement (CVL Certificate #23)
- Digital Signature Algorithm (DSA) key generation (required for Diffie-Hellman KAS): 1024 bits (Certificate #653)

In the FIPS mode of operation, the module implements the following non-Approved algorithms:

- A non-Approved Non-Deterministic Random Number Generator (NDRNG) to seed the DRBG
- The following commercially-available protocols for key establishment:
    - Transport Layer Security (TLS) 1.0/Secure Socket Layer (SSL) 3.1 protocol using RSA 2048 bits for key transport (key wrapping: key establishment methodology provides 112 bits of encryption strength)

In the non-FIPS mode of operation, the module also implements the non-Approved algorithms DES, MD5, RC4, and RSA-512, RSA-768, and RSA-1024 for signature generation and verification, and key establishment as well as the above listed protocols for key establishment.

2.3 Module Interfaces

FIPS 140-2 defines four logical interfaces:

- Data Input
- Data Output
- Control Input
- Status Output

The module features the following physical ports and LEDs:

- Serial port (RS232 DB9)
- Ethernet 10/100/1000 RJ-45 ports (Network Interface Card [NIC], quantity: 2)
- Monitor port (VGA DB15)
- Power input (100-240VAC)
- LEDs (four on the front panel and three on the rear panel)

The logical interfaces and their physical port mappings are described in Table 2.

Table 2 – Logical Interface and Physical Ports Mapping

Logical Interface	Physical Ports
Data Input	Serial, Ethernet
Data Output	Monitor, serial, Ethernet
Control Input	Serial, Ethernet
Status Output	Monitor, serial, Ethernet, LEDs

There are no ports on the front panel. There are four LEDs on the front panel. See Figure 3.

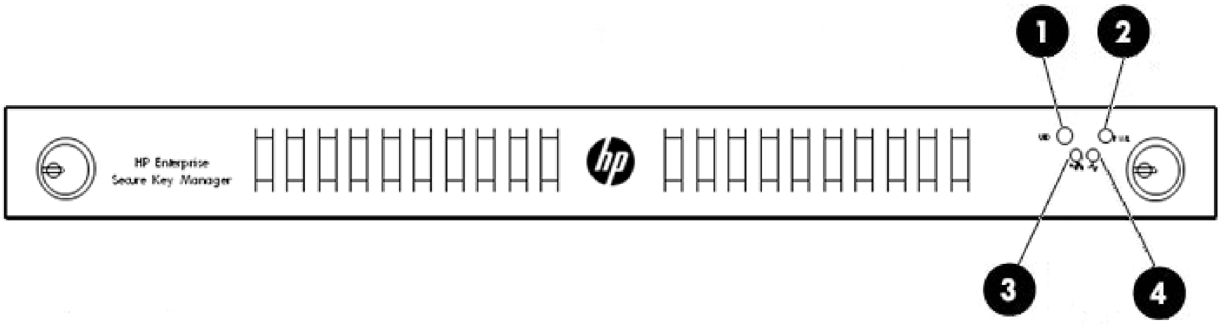

Figure 3 – Front Panel LEDs

Descriptions of the LEDs are given in Table 3.

Table 3 – Front Panel LED Definitions

Item	Description	Status
1	Unit Identifier (UID) LED/button	Blue = Identification is activated. Off = Identification is deactivated.
2	Power/Standby LED	Green = System is on. Amber = System is in standby, but power is still applied. Off = Power cord is not attached, power supply failure has occurred, no power supplies are installed, facility power is not available.
3	Aggregate Network LED	Solid green = Link to network Flashing green = Network activity Off = No network connection
4	System Health LED	Green = System health is normal. Amber = System health is degraded. Red = System health is critical. Off = System health is normal (when in standby mode).

The components on the rear panel are illustrated in

Figure 4.

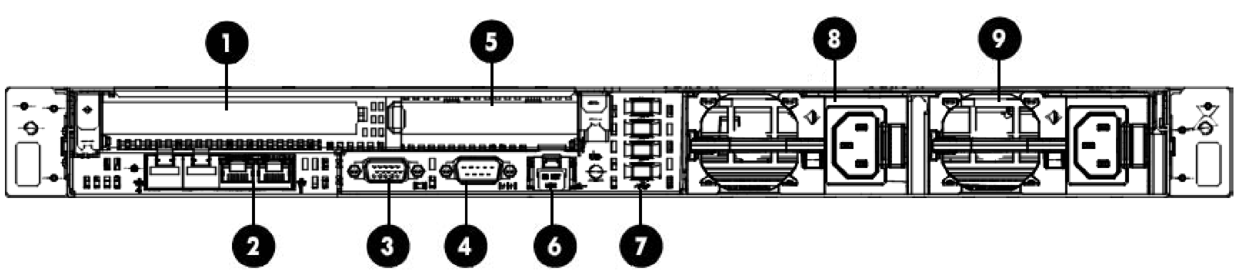

Figure 4 – Rear Panel Components

Descriptions of components on the rear panel are given in Table 4.

Table 4 – Rear Panel Components Descriptions

Item	Definition
1	Slot 2 PCIe 3.0 x 16 (Blocked)
2	NIC 4 connector (Disabled) NIC 3 connector (Disabled) NIC 2 connector NIC 1 connector
3	Video connector
4	Serial connector
5	Slot 1 PCIe 3.0 x 8 (Blocked)
6	iLO 3/NIC connector (Blocked)
7	USB connectors (4) (Blocked)
8	Power supply bay 2
9	Power supply bay 1

The three LEDs on the rear panel are illustrated in Figure 5.

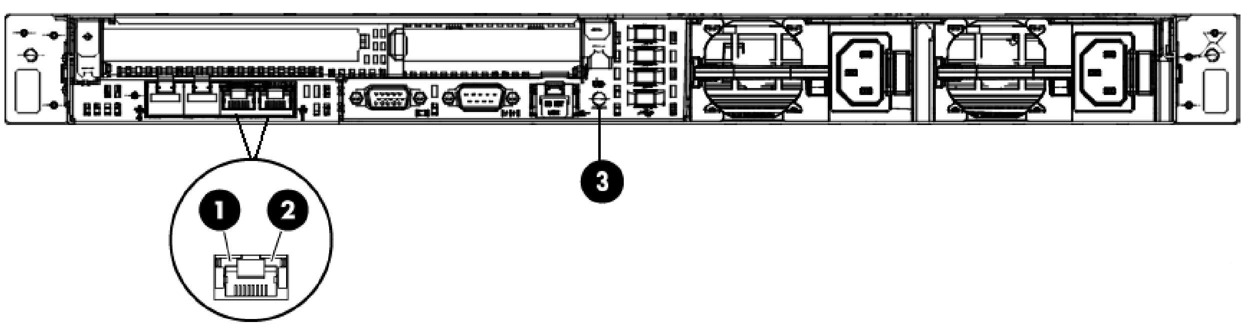

Figure 5 – Rear Panel LEDs

Descriptions of LEDs on the rear panel are given in Table 5.

Table 5 – Rear Panel LED Definitions

Item	Description	Status
1	Standard NIC activity LED for NIC 1 and NIC 2	Green = Activity exists. Flashing green = Activity exists. Off = No activity exists.
2	Standard NIC link LED for NIC 1 and NIC 2	Green = Link exists. Off = No link exists.
3	UID LED/button	Solid blue = Identification is activated. Off = Identification is deactivated.

2.4 Roles, Services, and Authentication

The module supports four authorized roles:

- Crypto-Officer
- User
- HP User
- Cluster Member

All roles require identity-based authentication.

2.4.1 Crypto-Officer Role

The Crypto-Officer accesses the module via the Web Management Console and/or the Command Line Interface (CLI). This role provides all services that are necessary for the secure management of the module. Table 6 shows the services for the Crypto-Officer role under the FIPS mode of operation. The purpose of each service is shown in the first column ("Service"), and the corresponding function is described in the second column ("Description"). The keys and Critical Security Parameters (CSPs) in the rightmost column correspond to the keys and CSPs introduced in Section 2.7.1.

Table 6 – Crypto-Officer Services

Service	Description	Keys/CSPs
Authenticate to ESKM	Authenticate to ESKM with a username and the associated password	Crypto-Officer passwords – read; TLS/SSH keys – read
Perform first-time initialization	Configure the module when it is used for the first time	Crypto-Officer (admin) password – write; Krsa private – write; Krsa private – write; Log signing RSA key – write; Log signature verification RSA key – write; KRsaPub – write; KRsaPriv – write.
Upgrade firmware	Upgrade firmware (firmware must be FIPS-validated)	Firmware upgrade key – read
Configure FIPS mode	Enable/disable FIPS mode	None
Manage keys	Manage all client keys that are stored within the module. This includes the generation, storage, export (only public keys), import, and zeroization of keys.	Client keys – write, read, delete; PKEK – write, read, delete.
Manage clusters	Manage all clusters that are defined within the module. This includes the creation, joining, and removal of a cluster from the module.	Cluster Member passwords – write, delete Cluster key –write, read, delete
Manage services	Manage all services supported by the module. This includes the starting and stopping of all services.	None
Manage operators	Create, modify, or delete module operators (Crypto-Officers and Users).	Crypto-Officer passwords – write, delete; User passwords – write, delete

Service	Description	Keys/CSPs
Manage certificates	Create/import/revoke certificates	KRsaPub – write, read, delete; KRsaPriv – write, read, delete; CARsaPub – write, read, delete; CARsaPriv – write, read, delete; Client RSA public keys – read.
Reset factory settings	Rollback to the default firmware shipped with the module	All keys/CSPs – delete
Restore default configuration	Delete the current configuration file and restores the default configuration settings	None
Restore configuration file	Restore a previously backed up configuration file	None
Backup configuration file	Back up a configuration file	None
Zeroize all keys/CSPs	Zeroize all keys and CSPs in the module	All keys and CSPs – delete

2.4.2 User Role

The User role is associated with external applications or clients that connect to the KMS via its XML interface. Users in this role may exercise services—such as key generation and management—based on configured or predefined permissions. See Table 7 for details. The keys and CSPs in the rightmost column correspond to the keys and CSPs introduced in Section 2.7.1.

Table 7 – User Services

Service	Description	Keys/CSPs
Authenticate to ESKM	Authenticate to ESKM with a username and the associated password	User passwords – read
Generate key	Generate a cryptographic key	Client keys – write; PKEK – write.
Modify key meta data	Change the key owner or update/add/delete the custom attributes	None
Delete key	Delete a cryptographic key	Client keys – delete; PKEK – delete.
Query key meta data	Output key names and meta data that the User is allowed to access	Client keys – read; PKEK – read.
Import key	Import key	Client keys – write; PKEK – write.
Export key	Export a cryptographic key	Client keys – read; PKEK – read.
Export certificate	Export a certificate	Client certificate – read
Get certificate info	Return a list of local CAs including the certificate status	None
Clone key	Clone an existing key under a different key name	Client keys – write, read; PKEK – write, read.
Generate random number	Generate a random number	DRBG seed – write, read, delete
Manage operators	Only users with administration permission can create, modify, or delete module operators	User passwords – write, delete
Sign certificate request	Only users with administration permission can sign certificate requests	Client RSA public key; CARsaPub – read; CARsaPriv – read.

2.4.3 HP User Role

The HP User role can reset the module to an uninitialized state in the event that all Crypto-Officer passwords are lost, or when a self-test permanently fails. See Table 8. The keys and CSPs in the rightmost column correspond to the keys and CSPs introduced in Section 2.7.1.

Table 8 – HP User Services

Service	Description	Keys/CSPs
Authenticate to the module	Authenticate to ESKM with a signed token	HP User RSA public key – read
Reset factory settings	Rollback to the default firmware shipped with the module	All keys/CSPs – delete
Restore default configuration	Delete the current configuration file and restores the default configuration settings	None
Zeroize all keys/CSPs	Zeroize all keys/CSPs in the module	All keys/CSPs – delete

2.4.4 Cluster Member Role

The Cluster Member role is associated with other ESKMs that can connect to this ESKM and access cluster services. See Table 9. The keys and CSPs in the rightmost column correspond to the keys and CSPs introduced in Section 2.7.1.

Table 9 – Cluster Member Services

Service	Description	Keys/CSPs
Authenticate Cluster Member	Authenticate to ESKM via TLS	Cluster Member passwords – read; Cluster key – read; Cluster Member RsaPub – read
Receive Configuration File	Update the module's configuration settings	None
Zeroize Key	Delete a specific key	Cluster key – delete
Backup Configuration File	Back up a configuration file	None

2.4.5 Authentication

The module performs identity-based authentication for the four roles. Two authentication schemes are used: authentication with certificate in TLS and authentication with password. See Table 10 for a detailed description.

Table 10 – Roles and Authentications

Role	Authentication
Crypto-Officer	Username and password with optional digital certificate
User	Username and password and/or digital certificate
HP User	Digital certificate
Cluster Member	Digital certificate

The 1024-bit RSA signature on a digital certificate provides 80-bits of security. There are 2^{80} possibilities. The probability of a successful random guess is 2^{-80}. Since $10^{-6} » 2^{-80}$, a random attempt is very unlikely to succeed. At least 80 bits of data must be transmitted for one attempt. (The actual number of bits that need to be transmitted for one attempt is much greater than 80. We are considering the worst case scenario. Note also that the 1024-bit signature verification option is only available to the User role; all other roles require 2048-bit digital certificates.) The processor used by the module has a working frequency of 2.5 gigabytes, hence, at most $60×2.5×10^9$ bits of data can be transmitted in 60 seconds. Since 80 bits are necessary for one attempt, at most $(60×2.5×10^9)/80 = 1.875×10^9$ attempts are possible in 60 seconds. However, there exist 2^{80} possibilities. $(1.875×10^9)/2^{80} = 1.55×10^{-15} « 10^{-5}$. The probability of a successful certificate attempt in 60 seconds is considerably less than 10^{-5}.

Passwords in the module must consist of eight or more characters from the set of 90 human-readable numeric, alphabetic (upper and lower case), and special character symbols. Excluding those combinations that do not meet password constraints (see Section 2.7.1 – Keys and CSPs), the size of the password space is about 60^8. The probability of a successful random guess is 60^{-8}. Since $10^{-6} » 60^{-8}$, a random attempt is very unlikely to succeed. After five unsuccessful attempts, the module will be locked down for 60 seconds; i.e., at most five trials are possible in 60 seconds. Since $10^{-5} » 5×60^{-8}$, the probability of a successful password attempt in 60 seconds is considerably less than 10^{-5}.

2.4.6 Unauthenticated Services

The following services do not require authentication:

- SNMP statistics
- FIPS status services
- Health check services
- Network Time Protocol (NTP) services
- Initiation of self-tests by rebooting the ESKM
- Negotiation of the XML protocol version for communications with the KMS

SNMP is used only for sending statistical information (SNMP traps). FIPS status and health check are status-report services, unrelated to security or cryptography. NTP is a date/time synchronization service that does not involve keys or CSPs. Initiation of self-tests and negotiation of the XML protocol version do not involve keys or CSPs.

The services listed above for each role comprise the entire set of services available in non-FIPS mode.

2.5 Physical Security

The module was tested and found conformant to the EMI/EMC requirements specified by Title 47 of the Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class A (that is, for business use).

The HP Enterprise Secure Key Manager is a multi-chip standalone cryptographic module. The entire contents of the module, including all hardware, software, firmware, and data, are enclosed in a metal case. The case is opaque and must be sealed using tamper-evident labels in order to prevent the case cover from being removed without signs of tampering. Two pick-resistant locks are installed on the module's front bezel to protect the front interfaces, including the power switch, from unauthorized access. All circuits in the module are coated with commercial standard passivation. Once the bezel is locked and the module has been configured to meet FIPS 140-2 Level 2 requirements, the module cannot be accessed without signs of tampering. See Section 3.3 – Physical Security Assurance of this document for more information.

2.6 Operational Environment

The operational environment requirements do not apply to the HP Enterprise Secure Key Manager—the module does not provide a general purpose operating system and only allows the updating of image components after checking an RSA signature on the new firmware image. Crypto-Officers can install a new firmware image on the ESKM by downloading the image to the ESKM. This image is signed by an RSA private key (which never enters the module). The ESKM verifies the signature on the new firmware image using the public key stored in the module. If the verification passes, the upgrade is allowed. Otherwise the upgrade process fails and the old image is reused.

2.7 Cryptographic Key Management

2.7.1 Keys and CSPs

The SSH and TLS protocols employed by the FIPS mode of the module are security-related. Table 11 and

Table 12 introduce cryptographic keys, key components, and CSPs involved in the two protocols, respectively.

Table 11 – List of Cryptographic Keys, Cryptographic Key Components, and CSPs for SSH

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
DH public param	2048-bit Diffie-Hellman public parameters	Generated by DRBG during session initialization	In plaintext	In volatile memory	Upon session termination	Negotiate SSH Ks and SSH Khmac
DH private param	256-bit Diffie-Hellman private parameters	Generated by DRBG during session initialization	Never	In volatile memory	Upon session termination	Negotiate SSH Ks and SSH Khmac
Krsa public	2048-bit RSA public keys	Generated by DRBG during first-time initialization	In plaintext	In non-volatile memory	At operator delete or zeroize request	Verify the signature of the server's message.
Krsa private	2048-bit RSA private keys	Generated by DRBG during first-time initialization	Never	In non-volatile memory	At operator delete or zeroize request	Sign the server's message.
SSH Ks	SSH session 168-bit TDES key, 128-, 192-, 256-bit AES key	Diffie-Hellman key agreement	Never	In volatile memory	Upon session termination or when a new Ks is generated (after a certain timeout)	Encrypt and decrypt data
SSH Khmac	SSH session 512-bit HMAC key	Diffie-Hellman key agreement	Never	In volatile memory	Upon session termination or when a new Khmac is generated (after a certain timeout)	Authenticate data

Notice that SSH version 2 is explicitly accepted for use in FIPS mode, according to section 7.1 of the NIST FIPS 140-2 Implementation Guidance.

Table 12 – List of Cryptographic Keys, Cryptographic Key Components, and CSPs for TLS

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
Pre-MS	TLS pre-master secret	Input in encrypted form from client	Never	In volatile memory	Upon session termination	Derive MS
MS	TLS master secret	Derived from Pre-MS using FIPS Approved key derivation function	Never	In volatile memory	Upon session termination	Derive TLS Ks and TLS Khmac
KRsaPub	Server RSA public key (2048-bit)	Generated by DRBG during first-time initialization	In plaintext a X509 certificate.	In non-volatile memory	At operator delete request	Client encrypts Pre-MS. Client verifies server signatures
KRsaPriv	Server RSA private key (2048-bit)	Generated by DRBG during first-time initialization	Never	In non-volatile memory	At operator delete or zeroize request	Server decrypts Pre-MS. Server generates signatures
CARsaPub	Certificate Authority (CA) RSA public key (2048-bit)	Generated by DRBG during first-time initialization	In plaintext	In non-volatile memory	At operator delete request	Verify CA signatures
CARsaPriv	CA RSA private key (2048-bit)	Generated by DRBG during first-time initialization	Never	In non-volatile memory	At operator delete or zeroize request	Sign server certificates
Cluster Member RsaPub	Cluster Member RSA public key (2048-bit)	Input in plaintext	Never	In volatile memory	Upon session termination	Verify Cluster Member signatures
TLS Ks	TLS session AES or TDES symmetric key(s)	Derived from MS	Never	In volatile memory	Upon session termination	Encrypt and decrypt data
TLS Khmac	TLS session HMAC key	Derived from MS	Never	In volatile memory	Upon session termination	Authenticate data

Table 13 details all cipher suites supported by the TLS protocol implemented by the module. The suite names in the first column match the definitions in RFC 2246 and RFC 4346.

Table 13 – Cipher Suites Supported by the Module's TLS Implementation in FIPS Mode

Suite Name	Authentication	Key Transport	Symmetric Cryptography	Hash
TLS_RSA_WITH_AES_256_CBC_SHA	RSA	RSA	AES (256-bit)	SHA-1
TLS_RSA_WITH_AES_128_CBC_SHA	RSA	RSA	AES (128-bit)	SHA-1
TLS_RSA_WITH_TDES_EDE_CBC_SHA	RSA	RSA	TDES (168-bit)	SHA-1

Other CSPs are tabulated in Table 14.

Table 14 – Other Cryptographic Keys, Cryptographic Key Components, and CSPs

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
Client AES key	128, 192 or 256-bit AES key	Generated by DRBG	Via TLS in encrypted form (encrypted with TLS Ks) per client's request	Encrypted in non-volatile memory	Per client's request or zeroize request	Encrypt plaintexts/decrypt ciphertexts
Client TDES key	TDES key	Generated by DRBG	Via TLS in encrypted form (encrypted with TLS Ks) per client's request	Encrypted in non-volatile memory	Per client's request or zeroize request	Encrypt plaintexts/decrypt ciphertexts
Client RSA public keys	RSA public key	Generated by DRBG	Via TLS in encrypted form (encrypted with TLS Ks) per client's request	Encrypted in non-volatile memory	At operator delete	Sign messages/verify signatures
Client RSA keys	RSA private keys	Generated by DRBG	Via TLS in encrypted form (encrypted with TLS Ks) per client's request	Encrypted in non-volatile memory	Per client's request or zeroize request	Sign messages/verify signatures
Client HMAC keys	HMAC keys	Generated by DRBG	Via TLS in encrypted form (encrypted with TLS Ks) per client's request	Encrypted in non-volatile memory	Per client's request or zeroize request	Compute keyed-MACs
Client certificate	X.509 certificate	Input in ciphertext over TLS	Via TLS in encrypted form (encrypted with TLS Ks) per client's request	In non-volatile memory	Per client's request or by zeroize request	Encrypt data/verify signatures
Crypto-Officer passwords	Character string	Input in ciphertext over TLS	Never	In non-volatile memory	At operator delete or by zeroize request	Authenticate Crypto-Officer
User passwords	Character string	Input in ciphertext over TLS	Never	In non-volatile memory	At operator delete or by zeroize request	Authenticate User
Cluster Member password	Character string	Input in ciphertext over TLS	Never	In non-volatile memory	At operator delete or zeroize request	When a device attempts to become a Cluster Member
HP User RSA public key	2048-bit RSA public key	Input in plaintext at factory	Never	In non-volatile memory	At installation of a patch or new firmware	Authenticate HP User
Cluster key	Character string	Input in ciphertext over TLS	Via TLS in encrypted form	In non-volatile memory	At operator delete or by zeroize request	Authenticate Cluster Member

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
Firmware upgrade key	2048-bit RSA public key	Input in plaintext at factory	Never	In non-volatile memory	When new firmware upgrade key is input	Used in firmware load test
Log signing keys	2048-bit RSA public and private keys	Generated by DRBG at first-time initialization	Never	In non-volatile memory	When new log signing keys are generated on demand by Crypto-Officer	Sign logs and verify signature on logs
DRBG seed	RNG seed	Generated by non-Approved RNG	Never	In non-volatile memory	When module is powered off	Initialize DRBG
PKEK	256-bit AES key	Generated by DRBG	In encrypted form for backup purposes only	In non-volatile memory	At operator delete or by zeroize request	Encrypt client keys

2.7.2 Key Generation

The module uses the DRBG (AES in CTR mode) as specified in SP 800-90A to generate cryptographic keys. This DRBG is a FIPS 140-2 Approved RNG as specified in Annex C to FIPS 140-2.

2.7.3 Key/CSP Zeroization

All ephemeral keys are stored in volatile memory in plaintext. Ephemeral keys are zeroized when they are no longer used. Other keys and CSPs are stored in non-volatile memory with client keys being stored in encrypted form.

To zeroize all keys and CSPs in the module, the Crypto-Officer should execute the reset factory settings zeroize command at the serial console interface. For security reasons, this command is available only through the serial console.

2.8 Self-Tests

The device implements two types of self-tests: power-up self-tests and conditional self-tests.

Power-up self-tests include the following tests:

- Firmware integrity tests (CRC-16 and RSA 2048-bit signature verification)
- Known Answer Test (KAT) on TDES
- KAT on AES
- KAT on SHA-1
- KAT on SHA-256
- KAT on SHA-384
- KAT on SHA-512
- KAT on HMAC SHA-1
- KAT on HMAC SHA-256
- KAT on DRBG
- KAT on Diffie-Hellman
- KAT on SSH Key Derivation Function
- KAT on RSA signature generation and verification

Conditional self-tests include the following tests:

- Pairwise consistency test for new RSA keys
- Continuous random number generator test on DRBG
- Continuous random number generator test on non-Approved RNG
- Firmware load test (RSA 2048-bit signature verification)
- Diffie-Hellman primitive test

The module has two error states: a Soft Error state and a Fatal Error state. When one or more power-up self-tests fail, the module may enter either the Fatal Error state or the Soft Error State. When a conditional self-test fails, the module enters the Soft Error state. See Section 3 of this document for more information.

2.9 Mitigation of Other Attacks

This section is not applicable. No claim is made that the module mitigates against any attacks beyond the FIPS 140-2 Level 2 requirements for this validation.

3 Secure Operation

The HP Enterprise Secure Key Manager meets Level 2 requirements for FIPS 140-2. The sections below describe how to place and keep the module in the FIPS mode of operation.

3.1 Initial Setup

The device should be unpacked and inspected according to the *Installation Guide*. The *Installation Guide* also contains installation and configuration instructions, maintenance information, safety tips, and other information.

3.2 Initialization and Configuration

3.2.1 First-Time Initialization

When the module is turned on for the first time, it will prompt the operator for a password for a default Crypto-Officer. The module cannot proceed to the next state until the operator provides a password that conforms to the password policy described in Section 2.7.1. The default username associated with the entered password is “admin”.

During the first-time initialization, the operator must configure minimum settings for the module to operate correctly. The operator will be prompted to configure the following settings via the serial interface:

- Date, Time, Time zone
- IP Address/Netmask
- Hostname
- Gateway
- Management Port

3.2.2 FIPS Mode Configuration

In order to comply with FIPS 140-2 Level 2 requirements, the following functionality must be disabled on the ESKM:

- Global keys
- File Transfer Protocol (FTP) for importing certificates and downloading and restoring backup files
- Lightweight Directory Access Protocol (LDAP) authentication
- Use of the following algorithms: RC4, MD5, DES, RSA-512, RSA-768, RSA-1024 (signature generation)
- SSL 3.0
- RSA encryption and decryption operations (note, however, that RSA encryption and decryption associated with TLS handshakes and Sign and Sign Verify *are* permitted)

These functions need not be disabled individually. There are two approaches to configuring the module such that it works in the Approved FIPS mode of operation:

Through a command line interface, such as SSH or serial console, the Crypto-Officer should use the fips compliant command to enable the FIPS mode of operation. This will alter various server settings as described above. See Figure 6. The fips server command is used for the FIPS status server configuration. The show fips status command returns the current FIPS mode configuration.

```
labhp (config)# fips compliant
This device is now FIPS compliant.
labhp (config)# fips server
Enable FIPS Status Server [y]:
Available IP addresses:
        1. All
        2. 192.168.0.202
Local IP (1-2)[1]:
Local Port [9081]:
labhp (config)# show fips status
FIPS Compliant: Yes
```

Figure 6 – FIPS Compliance in CLI

In the web administration interface, the Crypto-Officer should use the “High Security Configuration” page to enable and disable FIPS compliance. To enable the Approved FIPS mode of operation, click on the “Set FIPS Compliant” button. See Figure 7. This will alter various server settings as described above.

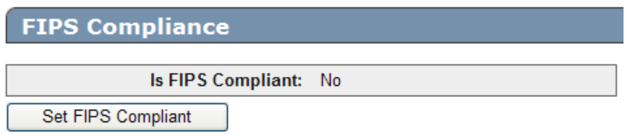

Figure 7 – FIPS Compliance in Web Administration Interface

In the web administration interface, the User can review the FIPS mode configuration by reading the “High Security Configuration” page.

The Crypto-Officer must zeroize all keys when switching from the Approved FIPS mode of operation to the non-FIPS mode and vice versa.

3.3 Physical Security Assurance

Five (5) serialized tamper-evidence labels have been applied during manufacturing on the metal casing. See Figure 8. The tamper-evidence labels have a special adhesive backing to adhere to the module’s surface and have an individual, unique serial number. They should be inspected periodically and compared to the previously-recorded serial number to verify that fresh labels have not been applied to a tampered module. If the labels show evidence of tamper, the Crypto-Officer should assume that the module has been compromised and contact HP Customer Support.

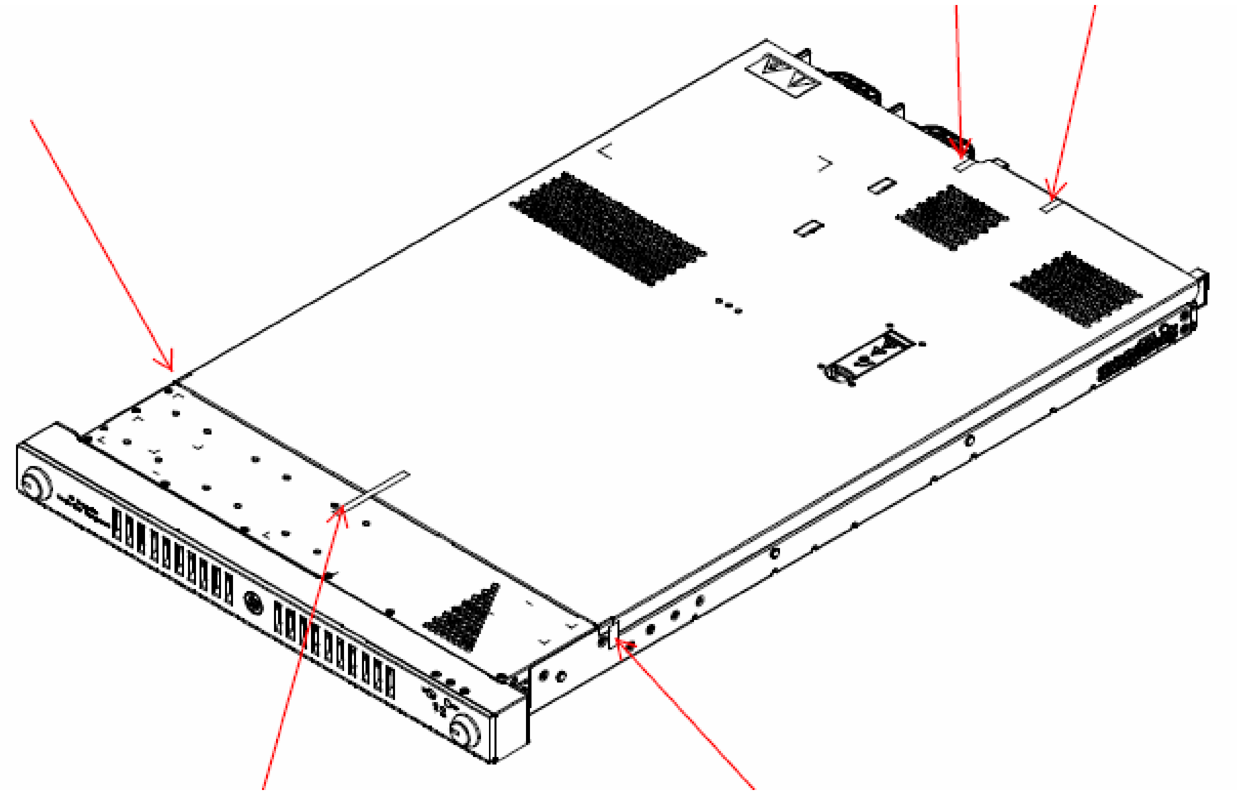

Figure 8 – Tamper-Evidence Labels (Qty. 5) on ESKM

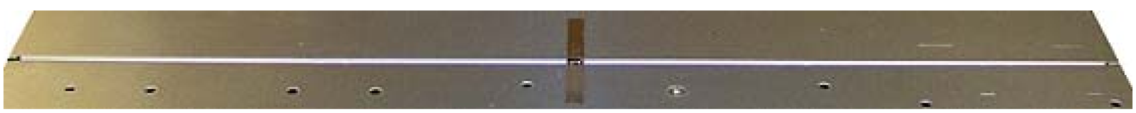

Figure 9 – Tamper-Evidence Label on top of ESKM

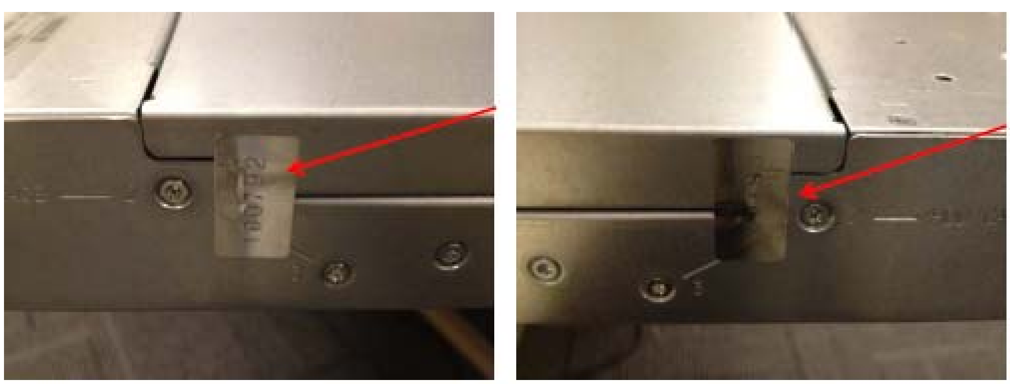

Figure 10 – Tamper-Evidence Labels on Side of ESKM

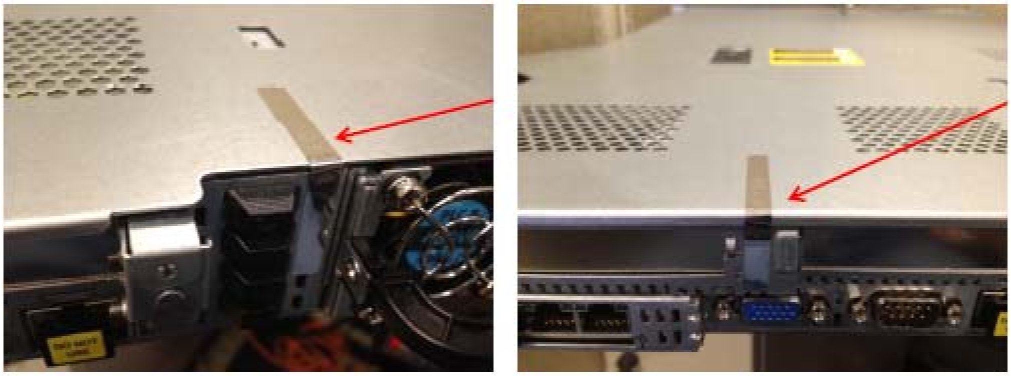

Figure 11 – Tamper-Evidence Labels on Rear of ESKM

3.4 Key and CSP Zeroization

To zeroize all keys and CSPs in the module, the Crypto-Officer should execute reset factory settings zeroize command in the serial console interface. Notice that, for security reasons, the command cannot be initiated from the SSH interface.

When switching between different modes of operations (FIPS and non-FIPS), the Crypto-Officer must zeroize all CSPs.

3.5 Error State

The module has two error states: a Soft Error state and a Fatal Error state.

When a power-up self-test fails, the module may enter either the Fatal Error state or the Soft Error State. When a conditional self-test fails, the module will enter the Soft Error state. The module can recover from the Fatal Error state if power is cycled or if the ESKM is rebooted. An HP User can reset the module when it is in the Fatal Error State. No other services are available in the Fatal Error state. The module can recover from the Soft Error state if power is cycled. With the exception of the firmware load test and Diffie-Hellman primitive test, the only service that is available in the Soft Error state is the FIPS status output via port 9081 (default). A User can connect to port 9081 and find the error message indicating the failure of FIPS self-tests. Access to port 9081 does not require authentication.

Acronyms

Table 15 – Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
ANSI	American National Standard Institute
BIOS	Basic Input/Output System
CA	Certificate Authority
CBC	Cipher Block Chaining
CLI	Command Line Interface
CMVP	Cryptographic Module Validation Program
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CSP	Critical Security Parameter
DES	Data Encryption Standard
DRBG	Deterministic Random Bit Generator
DSA	Digital Signature Algorithm
ECB	Electronic Codebook
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
ESKM	Enterprise Secure Key Manager
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
HDD	Hard Drive
HMAC	Keyed-Hash Message Authentication Code
HP	Hewlett-Packard
IDE	Integrated Drive Electronics
iLO	Integrated Lights-Out
I/O	Input/Output
IP	Internet Protocol
ISA	Instruction Set Architecture
KAT	Known Answer Test
KMS	Key Management Service
LDAP	Lightweight Directory Access Protocol
LED	Light Emitting Diode
MAC	Message Authentication Code
N/A	Not Applicable
NIC	Network Interface Card

Acronym	Definition
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
PCI	Peripheral Component Interconnect
RFC	Request for Comments
RNG	Random Number Generator
RSA	Rivest, Shamir, and Adleman
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSL	Secure Socket Layer
TDES	Triple Data Encryption Standard
TLS	Transport Layer Security
UID	Unit Identifier
USB	Universal Serial Bus
VGA	Video Graphics Array
XML	Extensible Markup Language