Hewlett Packard Enterprise

Enterprise Secure Key Manager

Hardware P/N C8Z61AA, Versions 4.0 [1] and 4.1 [2];
Firmware Versions: 6.0.0-51 [1] and 6.1.0-14 [2]

FIPS 140-2
Non-Proprietary Security Policy

Level 2 Validation

Document Version 1.2

March 29, 2016

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 Enterprise. 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 Enterprise Secure Key Manager.

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 and the Key Management Interoperability Protocol (KMIP) 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.

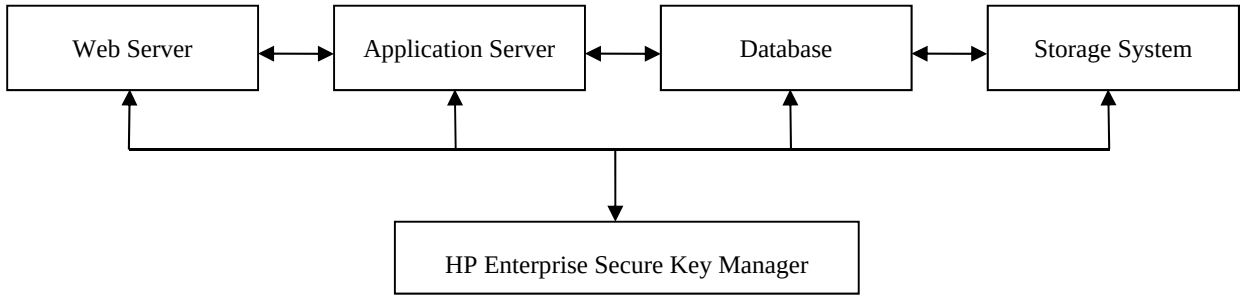

Figure 1 – Deployment Architecture of the HP Enterprise Secure Key Manager

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	2
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

Section	Section Title	Level
8	EMI/EMC	2
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.

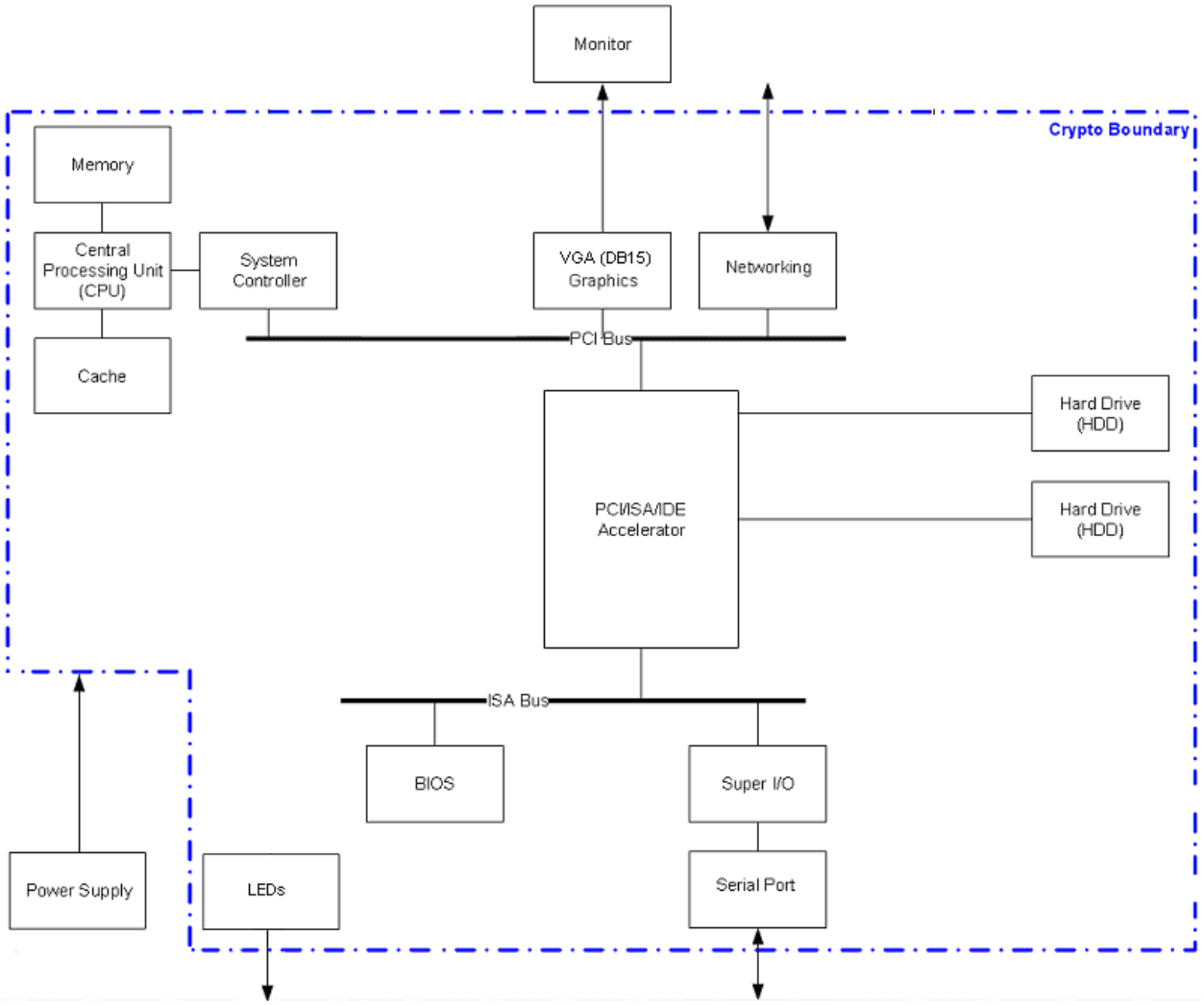

Figure 2 – Block Diagram of ESKM

2.2.1 FIPS Mode of Operation

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), Cipher Block Chaining (CBC), Counter (CTR), Galois/Counter Mode

(GCM)[1], Key Wrap (KW) modes, and 256 bits in Counter with CBC-MAC (CCM) (Certificates #3427 and #3428)
- Triple Data Encryption Standard (Triple-DES) encryption and decryption: 3-key, in ECB and CBC modes (Certificates #1932 and 1933)
- Secure Hash Algorithm (SHA)-1, SHA-224, SHA-256, SHA-384, SHA-512 (Certificates #2827 and #2828)
- Keyed-Hash Message Authentication Code (HMAC)-SHA-1, HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 (Certificates #2179 and #2180)
- Rivest, Shamir, and Adleman (RSA) American National Standard Institute (ANSI) X9.31 key generation, signature generation, and signature verification: 2048 and 3072bits (Certificates #1753 and #1754)
- RSA Decryption Primitive (RSADP) (CVL Certificates #518 and #521)
- TLS Key Derivation Function (KDF) (CVL Certificates #517 and #520)
- SSH KDF (CVL Certificates #519 and #522)
- Deterministic Random Bit Generator (DRBG) using AES in CTR mode for KMS (Certificates #827 and #829)
- Deterministic Random Bit Generator (DRBG) using AES in CTR mode for KMIP (Certificates #826 and #828)

In the FIPS mode of operation, the module implements the following non-Approved but allowed algorithms and protocols:

- A non-Approved Non-Deterministic Random Number Generator (NDRNG) to seed the DRBG
- The following commercially-available protocols for key establishment. The protocol algorithms have been tested by the CAVP (see certificate #s above) but the protocol implementations themselves have not been reviewed or tested by the CAVP or CMVP.
    - Transport Layer Security (TLS)/Secure Socket Layer (SSL) protocol using RSA 2048 bits for key transport (key wrapping: key establishment methodology provides 112 bits of encryption strength)
    - SSHv2 protocol using Diffie-Hellman key agreement (the Diffie-Hellman key establishment scheme provides 112 bits of security)

2.2.2 Non-FIPS Mode of Operation

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

- DES
- MD5
- RC4
- RSA-512, RSA-768, RSA-1024, and RSA-4096 for signature generation and verification, and key establishment as well as the above listed protocols for key establishment.
- SNMP v1/v2/v3 protocol. Any information sent over the SNMP protocol is considered plaintext status information.
- Non-Approved algorithms: HMAC (non-compliant), SHS (non-compliant), AES (non-compliant), Triple-DES (non-compliant), SNMP KDF (non-compliant), MD5, DES
- SSL 3.0 containing the following ciphersuites/algorithms:
    - SSL_RSA_WITH_3DES_EDE_CBC_SHA (enabled by default): RSA (non-compliant), Triple-DES (non-compliant), HMAC (non-compliant), SHS (non-compliant)

[1] If the module's power is lost and then restored, new GCM keys will be negotiated (to meet IG A.5).

- SSL_RSA_WITH_RC4_128_MD5 (disabled by default): RSA (non-compliant), RC4, HMAC (non-compliant), MD5
- SSL_RSA_WITH_RC4_128_SHA (disabled by default): RSA (non-compliant), MD5, HMAC (non-compliant), SHS (non-compliant)

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.

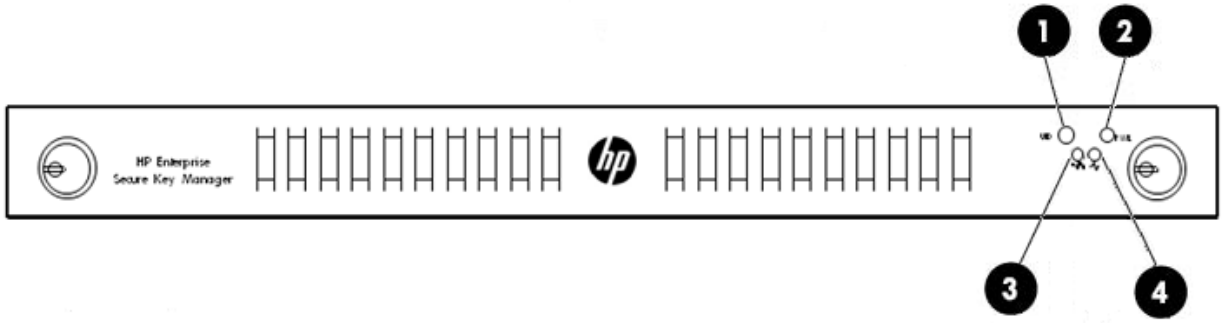

Figure 3 – Front Panel LEDs

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.

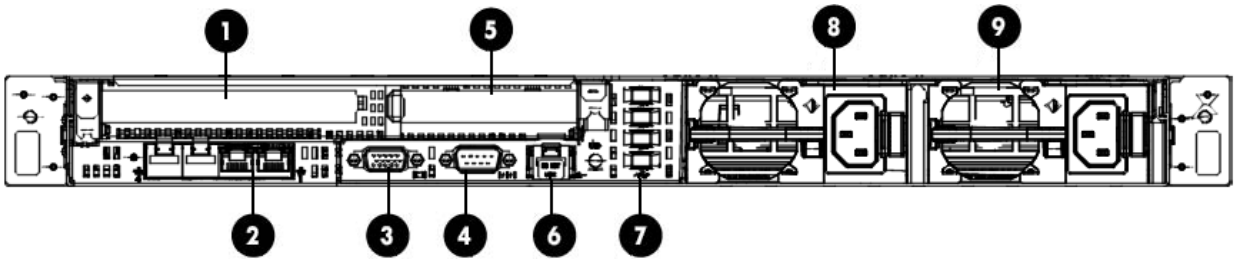

Figure 4 – Rear Panel Components

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)

Item	Definition
8	Power supply bay 2
9	Power supply bay 1

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

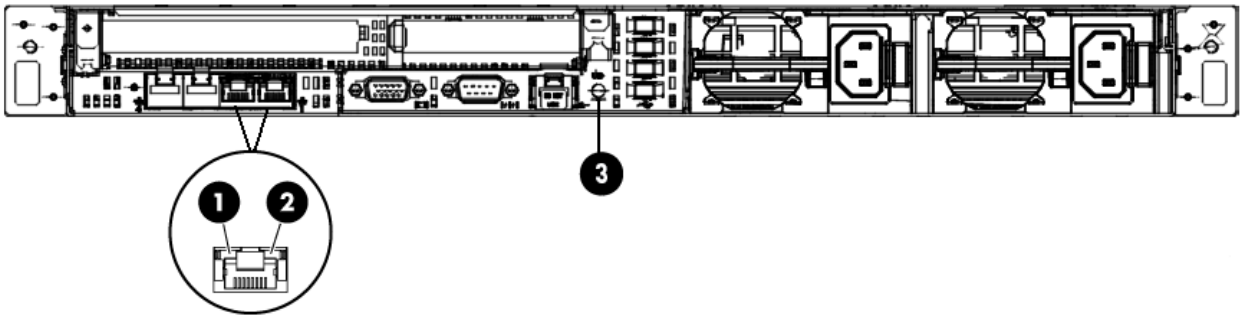

Figure 5 – Rear Panel LEDs

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 Critical Security Parameters (CSPs) in the rightmost column correspond to the keys and other 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.
Configure FIPS mode	Enable/disable FIPS mode	None
Manage CSPs	Manage all client CSPs that are stored within the module. This includes the generation, storage, export (only public keys), import, and zeroization of keys.	Client CSPs – 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
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 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 or to the KMIP 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 credentials such as username and password (in addition to the certificate during TLS)	User passwords – read.
Generate key	Generate a cryptographic key	Client keys – write; PKEK – write.
Modify CSP attributes	Update/add/delete attributes	None
Delete CSP	Delete a CSP	Client CSP – delete; PKEK – delete.
QueryCSP attributes	Query a CSP's attributes that the User is allowed to access	None
Query	Query the module's supported capabilities	None
Import CSP	Import CSPs such as keys, secret data	Client CSP – write; PKEK – write.
Export CSP	Export a CSP, such as a cryptographic key, certificate, and other KMIP objects	Client CSP – read; PKEK – read.
Get certificate info	Return a list of local CAs including the certificate status, certify and re-certify	None
Clone key	Clone an existing key under a different key name	Client CSP – write, read; PKEK – write, read.
Generate random number	Generate a random number	DRBG seed – write, read, delete
Crypto operation	Perform a cryptographic operation using the client key	Client key – write; PKEK – read.
Re-key	Create a new version of the client key	Client key – write; PKEK – read.
Activate CSP	Activate CSP	None
Revoke CSP	Revoke CSP	None

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	Username and password and Digital certificate

The 2048-bit RSA signature on a digital certificate provides 112-bits of security. There are 2^{112} possibilities. The probability of a successful random guess is 2^{-112}. Since $10^{-6} > 2^{-112}$, a random attempt is very unlikely to succeed. At least 112 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 112. We are considering the worst case scenario.) The processor used by the module has a working frequency of 2.5 gigabytes, hence, at most $60 \times 2.5 \times 10^9$ bits of data can be transmitted in 60 seconds. Since 112 bits are necessary for one attempt, at most $(60 \times 2.5 \times 10^9)/112 = 1.339 \times 10^9$ attempts are possible in 60 seconds. However, there exist 2^{112} possibilities. $(1.339 \times 10^9)/2^{112} = 2.58 \times 10^{-25} < 10^{-5}$. 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 $10^{-5} > 5 \times 60^{-8}$, 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. The module does NOT allow firmware upgrades in FIPS mode. If firmware is updated, the module is no longer a FIPS 140-2 Cryptographic Module.

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 3-key Triple-DES 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 Triple-DES 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	Triple-DES (3-key)	SHA-1
TLS_RSA_WITH_AES_128_CBC_SHA256	RSA	RSA	AES (128-bit)	SHA-256
TLS_RSA_WITH_AES_256_CBC_SHA256	RSA	RSA	AES (256-bit)	SHA-256

Suite Name	Authentication	Key Transport	Symmetric Cryptography	Hash
TLS_RSA_WITH_AES_128_GCM_SHA256	RSA	RSA	AES (128-bit)	SHA-256
TLS_RSA_WITH_AES_256_GCM_SHA384	RSA	RSA	AES (256-bit)	SHA-384

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	Triple-DES 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

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
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
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 or input in ciphertext over TLS	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 CSP

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 CSPs 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.

Since the zeroization process can take just over one minute, the Crypto-Officer must remain with the physical module until the zeroization operation is complete.

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 (RSA 2048-bit signature verification)
- Known Answer Test (KAT) on Triple-DES (encrypt and decrypt, ECB mode, 3-Key)
- KAT on AES (encrypt and decrypt, ECB mode, 128-bit key; this covers the KAT requirement for all AES modes although the GCM and Key Wrap modes are additionally tested)
- KAT on AES GCM (encrypt and decrypt, 256-bit key)

- KAT on AES Key Wrap (authenticated encryption and authenticated decryption, 128-, 192-, 256-bit key)
- KAT on HMAC (one KAT per SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512)
- KAT on SHA covered by above HMAC KATs per IG 9.1
- KAT on DRBG for KMS (CTR_DRBG, 256-bit AES with derivation function)
- KAT on DRBG for KMIP (CTR_DRBG, 256-bit AES with derivation function)
- KAT on Diffie-Hellman (2048-bit prime modules with 256-bit prime subgroup, shared secret calculation)
- KAT on SSH Key Derivation Function (2048-bit shared secret)
- KAT on TLS Key Derivation Function (TLS 1.0 with SHA-1, TLS 1.1 with SHA-256, TLS 1.1/1.2 with SHA-384)
- KAT on RSA signature generation and verification (sign, verify, encrypt, decrypt using 2048-bit key , SHA-256)
- KAT on RSA Decryption Primitive (decrypt, 2048-bit)

Conditional self-tests include the following tests:

- Pairwise consistency test for new RSA keys
- Continuous random number generator test on DRBG (for both KMS and KMIP)
- Health Checks per SP 800-90A Section 11.3 (for both KMS and KMIP)
- Continuous random number generator test on non-Approved RNG
- Diffie-Hellman pairwise consistency test
- 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 enters the Fatal 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
- 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.

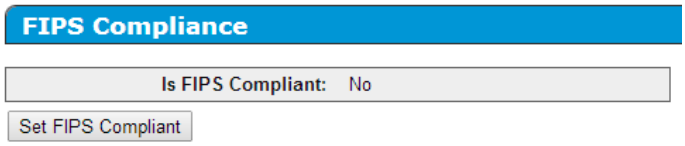

Figure 7 – FIPS Compliance in Web Administration Interface

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

When operating in a FIPS mode of operation, the following functionality is not allowed:

- 4096-bit RSA key generation
- 4096-bit Local CA certificate and certificate request generation
- 4096-bit signature generation and verification
- Firmware upgrades

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

All services are available in both the Approved FIPS mode of operation and the non-FIPS mode of operation.

3.3 Physical Security Assurance

Five 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 every six months 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.

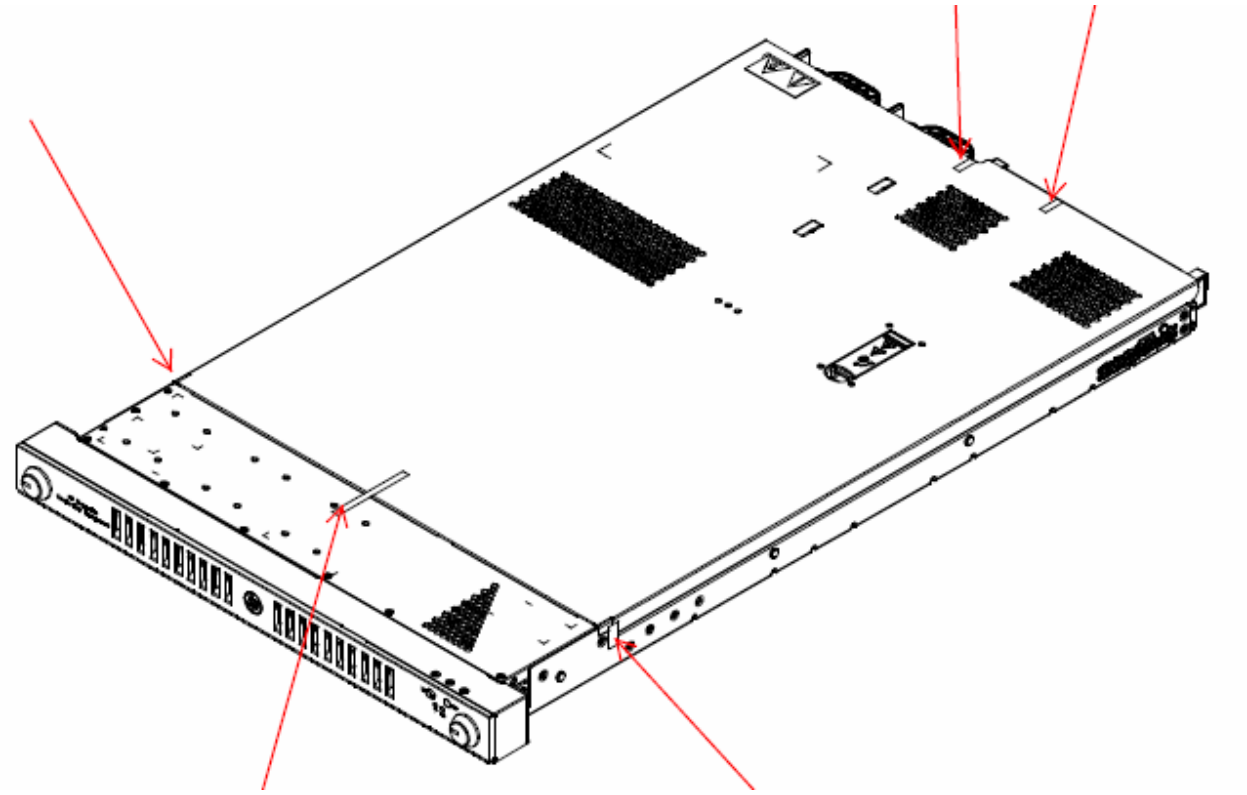

Figure 8 – Tamper-Evidence Labels on ESKM

Figure 9 – Tamper-Evidence Label on top of ESKM

Figure 10 – Tamper-Evidence Labels on Side of ESKM

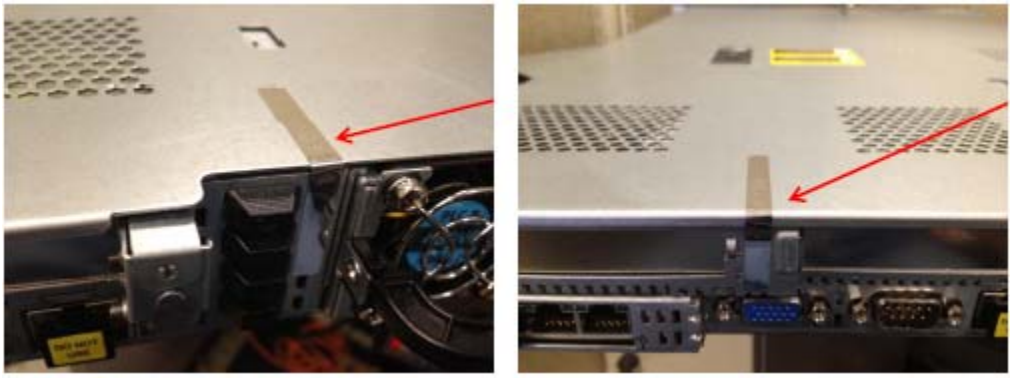

Figure 11 – Tamper-Evidence Labels on Rear of ESKM

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.

Since the zeroization process can take just over one minute, the Crypto-Officer must remain with the physical module until the zeroization operation is complete.

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 will enter the Fatal 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. 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
KMIP	Key Management Interoperability Protocol
LDAP	Lightweight Directory Access Protocol
LED	Light Emitting Diode
MAC	Message Authentication Code
N/A	Not Applicable

Acronym	Definition
NIC	Network Interface Card
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
Triple-DES	Triple Data Encryption Standard
TLS	Transport Layer Security
UID	Unit Identifier
USB	Universal Serial Bus
VGA	Video Graphics Array
XML	Extensible Markup Language