Hewlett-Packard Company

HP StorageWorks Secure Key Manager

(Hardware P/N AJ087A, Version 1.0; Firmware Version:1.0.1)

FIPS 140-2
Security Policy

Level 2 Validation

Document Version 1.0

Prepared for:	Prepared by:
Hewlett-Packard Company	**Corsec Security, Inc.**
19091 Pruneridge Ave. Cupertino, CA 95014	10340 Democracy Lane, Suite 201 Fairfax, VA 22030
Phone: (408) 447-3422 Fax: (408) 447-5525 http://www.hp.com	Phone: (703) 267-6050 Fax: (703) 267-6810 http://www.corsec.com

Revision History

Version	Modification Date	Modified By	Description of Changes
0.1	2007-10-02	Xiaoyu Ruan	Initial draft
0.2	2007-10-23	Xiaoyu Ruan	Revised addressing HP comments
0.3	2007-10-25	Xiaoyu Ruan	Revised addressing HP comments
0.4	2007-11-01	Xiaoyu Ruan	Minor formatting changes
0.5	2007-11-05	Xiaoyu Ruan	Sections 1 and 3 meet Level 3
0.6	2007-11-16	Xiaoyu Ruan	Addressed Lab comments
0.7	2007-11-19	Xiaoyu Ruan	Addressed Lab comments
0.8	2007-12-16	Xiaoyu Ruan	Addressed Lab comments
0.9	2007-12-18	Indra Fitzgerald Xiaoyu Ruan	Addressed Lab comments
1.0	2008-02-01	Indra Fitzgerald Xiaoyu Ruan	Addressed HP comments

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 StorageWorks Secure Key Manager (SKM) 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 SKM meets these requirements and how to use the SKM in a mode of operation compliant with FIPS 140-2. This policy was prepared as part of Level 2 FIPS 140-2 validation of the HP StorageWorks 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 StorageWorks Secure Key Manager is referred to as the *SKM*, 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.

1.3   Document Organization

The Security Policy is one document in a FIPS 140-2 submission package. The submission package also contains:

- Vendor Evidence
- Finite State Machine
- Other supporting documentation as additional references

This Security Policy and the other validation submission documentation have been produced by Corsec Security, Inc. under contract to HP. With the exception of this Security Policy, the FIPS 140-2 validation documentation is proprietary to HP and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact HP.

2 HP StorageWorks 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 StorageWorks 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 SKM for creation and management of cryptographic keys and related metadata.

Client applications can access the SKM 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 StorageWorks Secure Key Manager is shown in Figure 1 below.
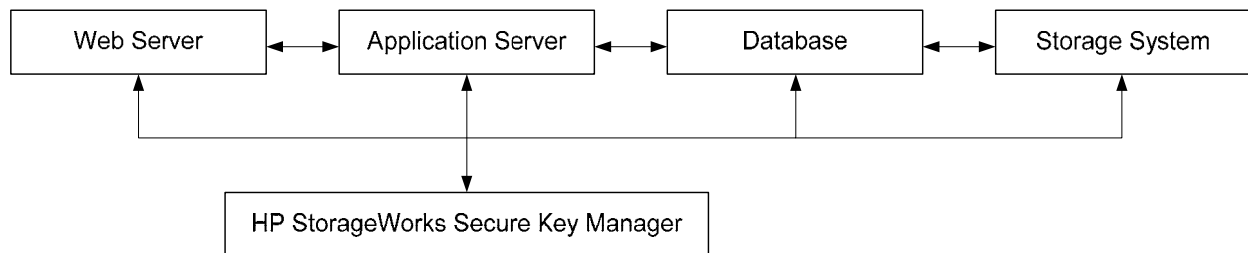
Figure 1 – Deployment Architecture of the HP StorageWorks Secure Key Manager

2.2 Cryptographic Module Specification

The HP StorageWorks Secure Key Manager is validated at FIPS 140-2 section levels shown in Table 1 – Security Level per FIPS 140-2 Section. Note that in this table, EMI and EMC mean Electromagnetic Interference and Electromagnetic Compatibility, respectively; N/A indicates "Not Applicable".

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
9	Self-Tests	2

Section	Section Title	Level
10	Design Assurance	2
11	Mitigation of Other Attacks	N/A

The block diagram of the module is given in Figure 2 – Block Diagram of SKM. The cryptographic boundary is clearly shown in the figure. Notice that power supply is not included in the boundary. In this figure, I/O means Input/Output, BIOS stands for Basic Input/Output System, LED stands for Light Emitting Diode, VGA stands for Video Graphics Array, PCI stands for Peripheral Component Interconnect, ISA stands for Instruction Set Architecture, and IDE represents Integrated Drive Electronics.
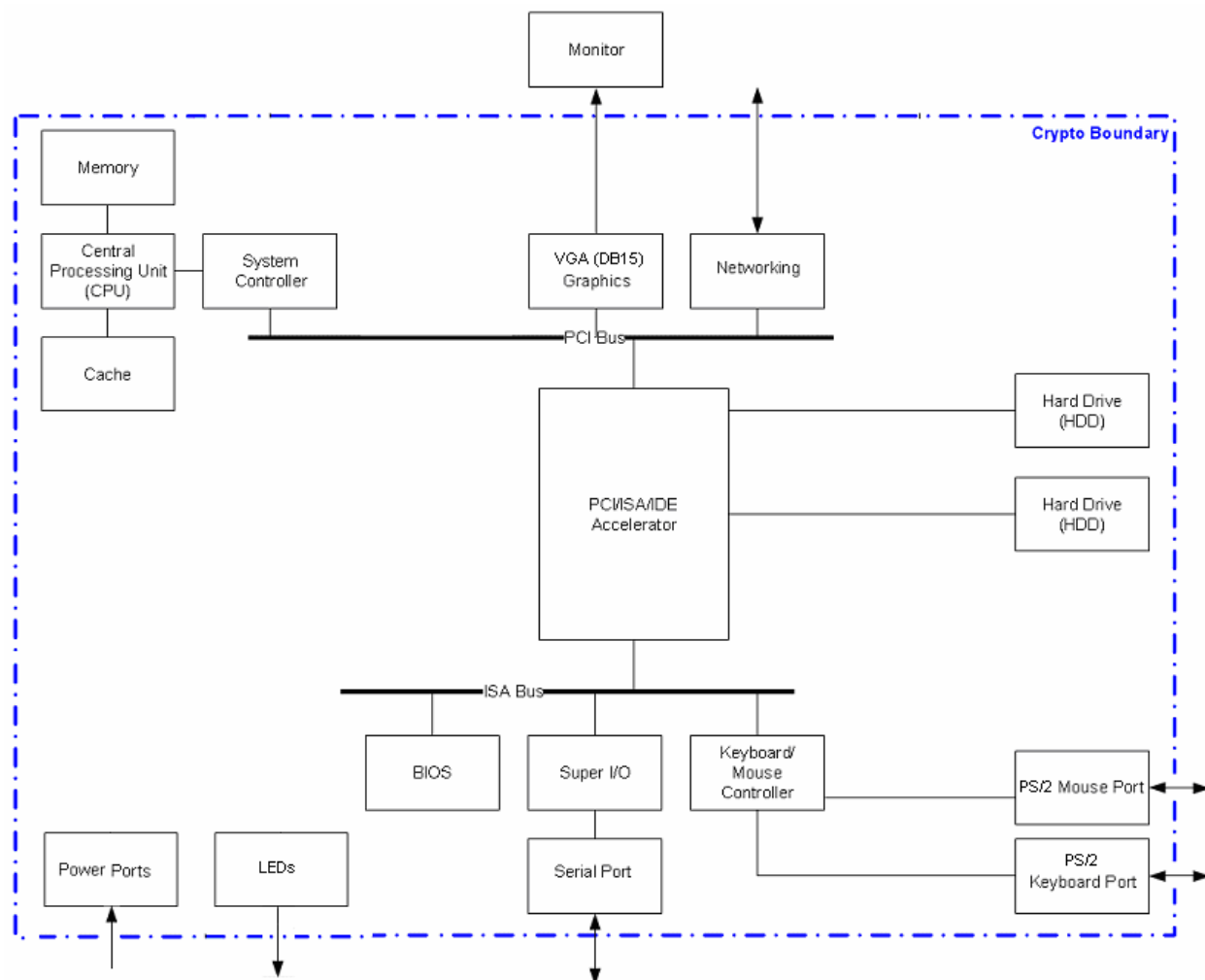
Figure 2 – Block Diagram of SKM

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 # 653)
- Triple Data Encryption Standard (3DES) encryption and decryption: 112 and 168 bits, in ECB and CBC modes (certificate # 604)
- Secure Hash Algorithm (SHA)-1 (certificate # 686)
- Keyed-Hash Message Authentication Code (HMAC)-SHA-1 (certificate # 338)

- Rivest, Shamir, and Adleman (RSA) American National Standard Institute (ANSI) X9.31 key generation, signature generation, and signature verification: 1024 and 2048 bits (certificate # 302)
- Digital Signature Algorithm (DSA) PQG generation, key generation, signature generation, and signature verification: 1024 bits (certificate # 244)
- ANSI X9.31 Appendix A.2.4 with 2-key 3DES Deterministic Random Number Generator (DRNG) (certificate # 375)

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

- A non-approved Random Number Generator (RNG) to seed the ANSI X9.31 DRNG
- The following commercially-available protocols for key establishment:
    o Transport Layer Security (TLS) 1.0/ Secure Socket Layer (SSL) 3.1 protocol using RSA 1024 and 2048 bits for key transport. Caveat: The RSA 1024- and 2048-bit key wrapping and key establishment provide 80 and 112 bits of encryption strength, respectively.
    o SSHv2 protocol using Diffie-Hellman key agreement. Caveat: The Diffie-Hellman key establishment scheme provides 80 bits of encryption strength.

In the non-FIPS mode of operation, the module implements the non-approved functions described above in addition to Data Encryption Standard (DES), MD5, RC4, RC2, and 512- and 768-bit RSA for signature generation and verification, and 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)
- Mouse port (PS/2)
- Keyboard port (PS/2)
- Monitor port (VGA DB15)
- Power ports (power bay #1 and power bay #2)
- LEDs (six on the front panel and five on the rear panel)
  Note: Two additional LEDs are located on the module's dual removable power supplies, which are outside the cryptographic boundary.

The logical interfaces and their physical port mappings are described in Table 2 – Logical Interface and Physical Ports Mapping.

Table 2 – Logical Interface and Physical Ports Mapping

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

There are no buttons or ports on the front panel. There are six LEDs on the front panel. See Figure 3 – Front Panel LEDs.
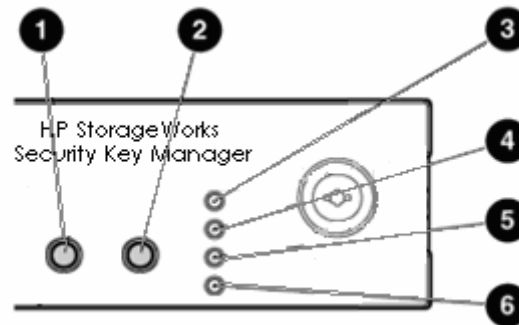
Figure 3 – Front Panel LEDs

Descriptions of the LEDs are given in Table 3 – Front Panel LED Definitions.

Table 3 – Front Panel LED Definitions

Item	Description	Status
1	Power On/Standby button and system power LED	Green = System is on. Amber = System is shut down, 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, or disconnected power button cable.
2	Unit Identifier (UID) button/LED	Blue = Identification is activated. Off = Identification is deactivated.
3	Internal health LED	Green = System health is normal. Amber = System health is degraded. To identify the component in a degraded state, refer to "HP Systems Insight Display and LEDs". Red = System health is critical. To identify the component in a critical state, refer to "HP Systems Insight Display and LEDs". Off = System health is normal (when in standby mode).
4	External health LED (power supply)	Green = Power supply health is normal. Amber = Power redundancy failure occurred. Off = Power supply health is normal when in standby mode.
5	NIC 1 link/activity LED	Green = Network link exists. Flashing green = Network link and activity exist. Off = No link to network exists. If power is off, the front panel LED is not active. View the LEDs on the RJ-45 connector for status by referring to the rear panel LEDs.
6	NIC 2 link/activity LED	Green = Network link exists. Flashing green = Network link and activity exist. Off = No link to network exists. If power is off, the front panel LED is not active. View the LEDs on the RJ-45 connector for status by referring to the rear panel LEDs

The components on the rear panel are illustrated in Figure 4 – Rear Panel Components.
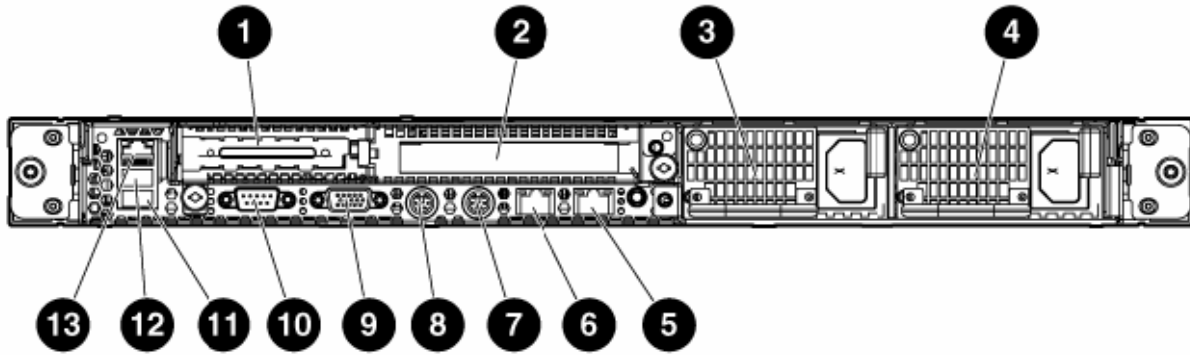
Figure 4 – Rear Panel Components

Descriptions of components on the rear panel are given in Table 4 – Rear Panel Components Descriptions.

Table 4 – Rear Panel Components Descriptions

Item	Definition
1	PCI Express expansion slot 1 (Blocked)
2	PCI Express expansion slot 2 (Blocked)
3	Power supply bay 2
4	Power supply bay 1
5	NIC connector 1 (Ethernet)
6	NIC connector 2 (Ethernet)
7	Keyboard connector
8	Mouse connector
9	Video connector
10	Serial connector
11	Universal Serial Bus (USB) connector 1 (Blocked)
12	USB connector 2 (Blocked)
13	Integrated Lights-Out (iLO) 2 NIC connector (Blocked)

The seven LEDs on the rear panel are illustrated in Figure 5 – Rear Panel LEDs.
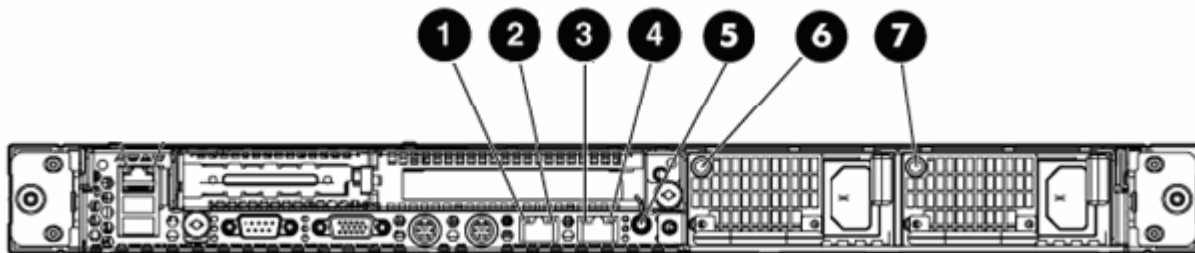

Figure 5 – Rear Panel LEDs

Descriptions of LEDs on the rear panel are given in Table 5 – Rear Panel LED Definitions. Notice that the power supplies are not included in the cryptographic boundary. The two power supply LEDs (items 6 and 7 in Table 5) are not part of the module's status output interface.

Table 5 – Rear Panel LED Definitions

Item	Description	Status
1	10/100/1000 NIC 1 activity LED	Green = Activity exists. Flashing green = Activity exists. Off = No activity exists.
2	10/100/1000 NIC 1 link LED	Green = Link exists. Off = No link exists.
3	10/100/1000 NIC 2 activity LED	Green = Activity exists. Flashing green = Activity exists. Off = No activity exists.
4	10/100/1000 NIC 2 link LED	Green = Link exists. Off = No link exists.
5	UID LED	Blue = Identification is activated. Off = Identification is deactivated.
6	Power supply 2 LED	Green = Normal Off = System is off or power supply has failed
7	Power supply 1 LED	Green = Normal Off = System is off or power supply has failed

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 SKM	Authenticate to SKM with a username and the associated password	Crypto Officer passwords – read; GuiClientRsaPub – read

Service	Description	Keys/CSPs
Perform first-time initialization	Configure the module when it is used for the first time	Crypto Officer (admin) password – write; Kdsa public/private – 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
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
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 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 – User Services 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 SKM	Authenticate to SKM with a username and the associated password	User passwords – read
Generate key	Generate a cryptographic key	Client keys – 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
Query key meta data	Output the following key information that the User is allowed to access: key length, whether a key is exportable, whether a key can be deleted by current user, key permissions, supported algorithms and modes for a key, and the custom attributes.	Client keys – read
Query key names	Output the list of key names and meta data that the User is allowed to access	Client keys – read
Import key	Import key	Client keys – write
Export key	Export a cryptographic key	Client keys – read
Export Certificate	Export a certificate	Client certificate - read
Clone Key	Clone an existing key under a different key name	Client keys – write, read
Generate random number	Generate a random number	ANSI X9.31 DRNG seed – write, read, delete
Encrypt data	Encrypt plaintext with AES or 3DES	Client AES/3DES key – read
Decrypt data	Decrypt ciphertext with AES or 3DES	Client AES/3DES key – read
Sign message with RSA	Sign a message with RSA	Client RSA keys – read
Verify RSA signature	Verify an RSA signature	Client RSA keys – read
MAC data	Compute Message Authentication Code (MAC) of data	Client HMAC key – read
Verify MAC	Verify MAC of data	Client HMAC key – read
Manage operators	Only users with administration permission can create, modify, or delete module operators	User passwords – write, delete

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 – HP User Services. 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 SKM 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 SKMs that can connect to this SKM and access cluster services. See Table 9 – Cluster Member Services. 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 SKM 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 – Roles and Authentications 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 over TLS

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 $10^{-6} \gg 2^{-80}$, 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.) The processor used by the module has a working frequency of 3.0 gigabytes, hence, at most $60 \times 3.0 \times 10^9$ bits of data can be transmitted in 60 seconds. Since 80 bits are necessary for one attempt, at most $(60 \times 3.0 \times 10^9)/80 = 2.25 \times 10^9$ attempts are possible in 60 seconds. However, there exist 2^{80} possibilities. $(2.25 \times 10^9)/2^{80} = 1.86 \times 10^{-15} \ll 10^{-5}$. 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 $10^{-6} \gg 60^{-8}$, a random attempt is very unlikely to succeed. After six unsuccessful attempts, the module will be locked down for 60 seconds; i.e., at most six trials are possible in 60 seconds. Since $10^{-5} \gg 6 \times 60^{-8}$, 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 SKM
- 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.

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 StorageWorks 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. The case front bezel contains two pick-resistant locks to prevent unauthorized access to the module's components. All circuits in the module are coated with commercial standard passivation. Once 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 StorageWorks 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 SKM by downloading the image to the SKM. This image is signed by an RSA private key (which never enters the module). The SKM 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 – List of Cryptographic Keys, Cryptographic Key Components, and CSPs for SSH and Table 12 – List of Cryptographic Keys, Cryptographic Key Components, and CSPs for TLS, 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	1024-bit Diffie-Hellman public parameters	Generated by ANSI X9.31 DRNG during session initialization	In plaintext	In volatile memory	Upon session termination	Negotiate SSH Ks and SSH Khmac
DH private param	1024-bit Diffie-Hellman private parameters	Generated by ANSI X9.31 DRNG during session initialization	Never	In volatile memory	Upon session termination	Negotiate SSH Ks and SSH Khmac
Kdsa public	1024-bit DSA public keys	Generated by ANSI X9.31 DRNG during first-time initialization	In plaintext	In non-volatile memory	At operator delete or zeroize request	Verify the signature of the server's message.
Kdsa private	1024-bit DSA private keys	Generated by ANSI X9.31 DRNG during first-time initialization	Never	In non-volatile memory	At operator delete or zeroize request	Sign the server's message.
Krsa public	1024-bit RSA public keys	Generated by ANSI X9.31 DRNG 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	1024-bit RSA private keys	Generated by ANSI X9.31 DRNG 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 3DES 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	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	Authenticate data

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

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
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 (1024- or 2048-bit)	Generated by ANSI X9.31 DRNG 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 (1024- or 2048-bit)	Generated by ANSI X9.31 DRNG 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 (1024- or 2048-bit)	Generated by ANSI X9.31 DRNG during first-time initialization	In plaintext	In non-volatile memory	At operator delete request	Verify CA signatures
CARsaPriv	CA RSA private key (1024- or 2048-bit)	Generated by ANSI X9.31 DRNG during first-time initialization	never	In non-volatile memory	At operator delete or zeroize request	Sign server certificates
GuiClientRsaPub	GUI Client RSA public key (1024- or 2048-bit)	Input in plaintext	never	In volatile memory	Upon session termination	Verify GUI Client signatures
Cluster Member RsaPub	Cluster Member RSA public key (1024- or 2048-bit)	Input in plaintext	Never	In volatile memory	Upon session termination	Verify Cluster Member signatures
TLS Ks	TLS session AES or 3DES 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_3DES_EDE_CBC_SHA	RSA	RSA	3DES (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 ANSI X9.31 DRNG	Via TLS in encrypted form (encrypted with TLS Ks) per client's request	In non-volatile memory	Per client's request or zeroize request	Encrypt plaintexts/decrypt ciphertexts
Client 3DES key	3DES key	Generated by ANSI X9.31 DRNG	Via TLS in encrypted form (encrypted with TLS Ks) per client's request	In non-volatile memory	Per client's request or zeroize request	Encrypt plaintexts/decrypt ciphertexts
Client RSA public key	RSA public key	Generated by ANSI X9.31 DRNG	Via TLS in encrypted form (encrypted with TLS Ks) per client's request	In non-volatile memory	At operator delete	Verify signatures
Client RSA private key	RSA private keys	Generated by ANSI X9.31 DRNG	Via TLS in encrypted form (encrypted with TLS Ks) per client's request	In non-volatile memory	Per client's request or zeroize request	Sign messages
Client HMAC key	HMAC keys	Generated by ANSI X9.31 DRNG	Via TLS in encrypted form (encrypted with TLS Ks) per client's request	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	Verify signatures
Crypto Officer passwords	Character string	Input in plaintext	Never	In non-volatile memory	At operator delete or by zeroize request	Authenticate Crypto Officer
User passwords	Character string	Input in plaintext	Never	In non-volatile memory	At operator delete or by zeroize request	Authenticate User

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
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	Never	In non-volatile memory	At operator delete or by zeroize request	Authenticate Cluster Member
Firmware upgrade key	1024-bit RSA public key	Input in plaintext at factory	Never	In non-volatile memory	When new firmware upgrade key is input	Used in firmware upgrade integrity test
Log signing keys	1024-bit RSA public and private keys	Generated by ANSI X9.31 DRNG at first-time initialization	Never	In non-volatile memory	When new log signing keys are generated on demand by Crypto Officer or by zeroize request	Sign logs and verify signature on logs
ANSI X9.31 DRNG seed	DRNG seed	Generated by non-Approved RNG	Never	In non-volatile memory	When module is powered off	Initialize ANSI X9.31 DRNG

2.7.2   Key Generation

The module uses an ANSI X9.31 DRNG with 2-key 3DES to generate cryptographic keys. This DRNG is a FIPS 140-2 approved DRNG as specified in Annex C to FIPS PUB 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.

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 eight tests:

- Firmware integrity tests
- Known Answer Test (KAT) on 3DES
- KAT on AES
- KAT on SHA-1
- KAT on HMAC-SHA-1
- KAT on ANSI X9.31 DRNG
- KAT on RSA signature generation and verification

- Pairwise consistency test on DSA signature generation and verification

Conditional self-tests include the following five tests:

- Pairwise consistency test for new DSA keys
- Pairwise consistency test for new RSA keys
- Continuous random number generator test on ANSI X9.31 DRNG
- Continuous random number generator test on non-Approved RNG
- Firmware upgrade integrity 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 StorageWorks 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 *User Guide*. The *User Guide* also contains installation and configuration instructions, maintenance information, safety tips, and other information. The device itself must be affixed with tamper-evident labels that are included in the packaging. See Figure 9 – Tamper-Evidence Labels for locations of tamper-evidence labels.

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 SKM:

- 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, RC2, MD5, DES, RSA-512, RSA-768
- SSL 2.0 and SSL 3.0
- Hot-swappable drive capability
- 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 (synonymous with Configure FIPS mode command) to enable the FIPS mode of operation. This will alter various server settings as described above. See Figure 6 – FIPS Compliance in CLI. 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 – FIPS Compliance in Web Administration Interface. This will alter various server settings as described above.
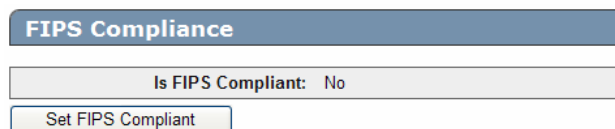
FIPS Compliance

Is FIPS Compliant: No

Set FIPS Compliant

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. See Figure 8 – High Security Configuration in Web Administration Interface.

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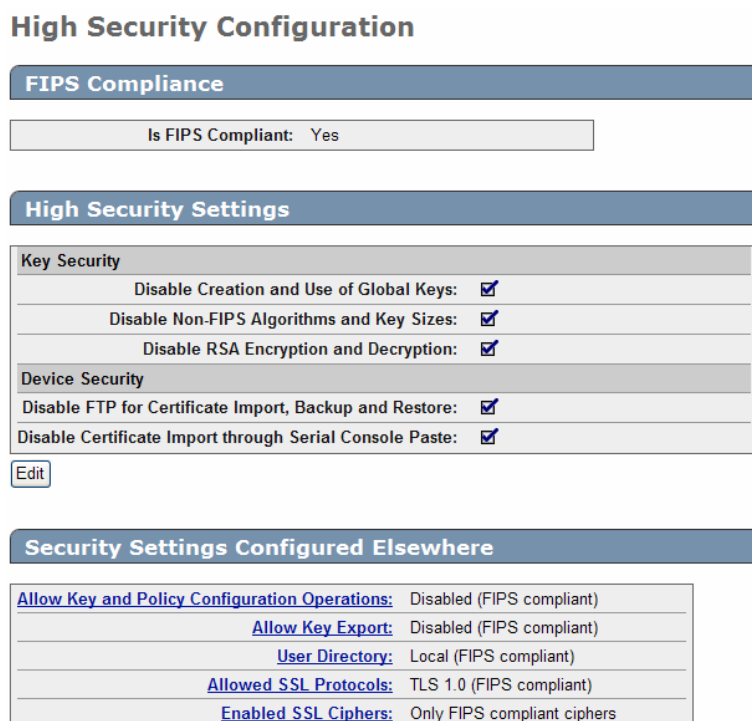
High Security Configuration

FIPS Compliance

Is FIPS Compliant: Yes

High Security Settings

Key Security

Disable Creation and Use of Global Keys:	☑
Disable Non-FIPS Algorithms and Key Sizes:	☑
Disable RSA Encryption and Decryption:	☑

Device Security

Disable FTP for Certificate Import, Backup and Restore:	☑
Disable Certificate Import through Serial Console Paste:	☑

Edit

Security Settings Configured Elsewhere

Allow Key and Policy Configuration Operations:	Disabled (FIPS compliant)
Allow Key Export:	Disabled (FIPS compliant)
User Directory:	Local (FIPS compliant)
Allowed SSL Protocols:	TLS 1.0 (FIPS compliant)
Enabled SSL Ciphers:	Only FIPS compliant ciphers

Figure 8 – High Security Configuration in Web Administration Interface

3.3 Physical Security Assurance

Serialized tamper-evidence labels have been applied at two locations on the metal casing. See Figure 9 – Tamper-Evidence Labels. The tamper-evidence labels have a special adhesive backing to adhere to the module's painted surface. The tamper-evidence labels have individual, unique serial numbers. They should be inspected periodically and compared to the previously-recorded serial numbers to verify that fresh labels have not been applied to a tampered module. The module also utilizes pick resistant locks on the front bezel to protect against unauthorized access to the module's components.
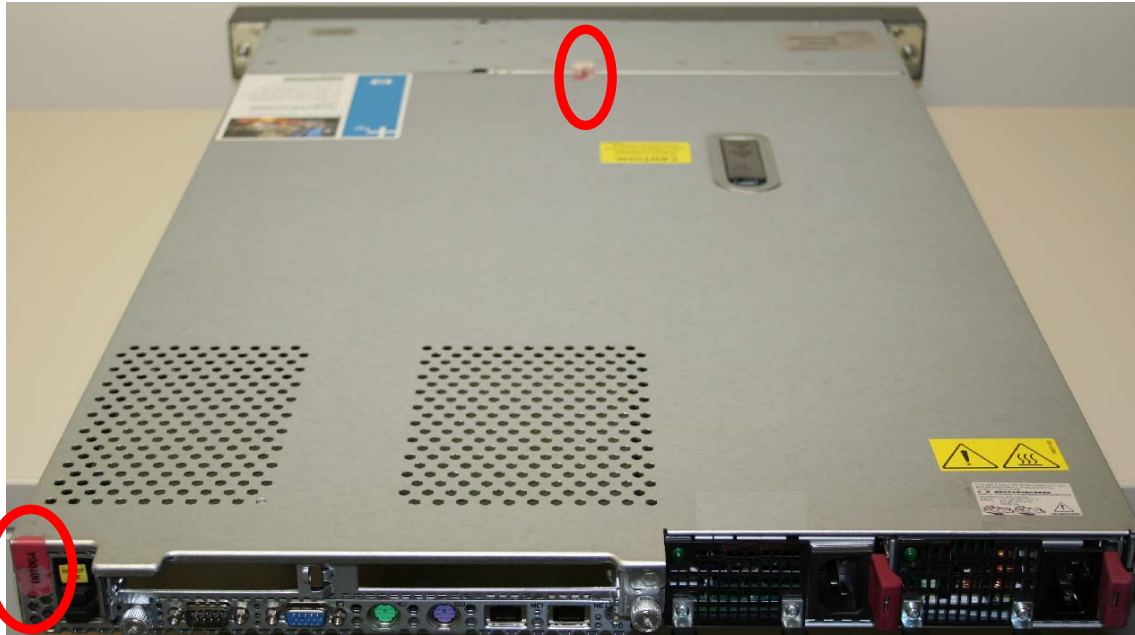
Figure 9 – Tamper-Evidence Labels

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 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 an HP User resets the module. No other services (other than FIPS status output) are available in the Fatal Error state. The module can recover from the Soft Error state only if power is cycled. 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. See Figure 10 – FIPS Status Report for a screenshot of the FIPS status report.

FIPS Status Report

Product:	HP StorageWorks Secure Key Manager
Box ID:	USE723N59N
Hostname:	labhp
IP Address(es):	192.168.0.202
Device State:	normal
FIPS Compliant:	yes

Test Results:

AES Encryption	success at Mon Oct 15 10:39:40 2007
DES Encryption	success at Mon Oct 15 10:39:40 2007
DSA Encryption	success at Mon Oct 15 10:39:40 2007
HMAC Algorithm	success at Mon Oct 15 10:39:40 2007
SHA1 Algorithm	success at Mon Oct 15 10:39:40 2007
RSA Encryption	success at Mon Oct 15 10:39:40 2007
X9.31 PRNG	success at Mon Oct 15 10:39:40 2007
Continuous Random Number Generation	success at Mon Oct 15 18:57:03 2007
RSA Pairwise Consistency	success at Mon Oct 15 15:42:41 2007
DSA Pairwise Consistency	success at Mon Oct 15 15:42:42 2007
Software Integrity	success at Mon Oct 15 10:40:06 2007

Figure 10 – FIPS Status Report

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