Red Hat Enterprise Linux 5 OpenSSH Server Cryptographic Module v1.0

FIPS 140-2 Security Policy

version 1.3

Last Update: 2010-06-16

Contents

Document History

Version	Date of Change	Author	Changes to Previous Version
0.1	2008-09-18	SHW - atsec	Initial
0,2	2008-10-16	SHW - atsec	Draft
1,0	2008-10-26	SHW - atsec	First release
1,1	2010-03-15	SHW - atsec	Version update
1,2	2010-04-13	SHW - atsec	Single user mode
1,3	2010-06-16	SHW - atsec	Correct RSA CAVS certificate number

1 Cryptographic Module Specification (140-2 Section 4.1)

This document is the non-proprietary security policy for the OpenSSH FIPS Object Module, and was prepared as part of the requirements for conformance to Federal Information Processing Standard (FIPS) 140-2, Level 1 .

The following section describes the module and how it complies with the FIPS 140-2 standard in each of the required areas.

1.1 Description of Module

The OpenSSH module is a software only, security level 1 cryptographic module, running on a multi-chip standalone platform. The module supplies cryptographic support for the SSH protocol or the Red Hat Enterprise Linux user space. The RPM version for the validated module is 4.3p2-36.el5_4.4.

All cryptographic operations and the module integrity check are performed by the Red Hat Enterprise Linux OpenSSL Cryptographic Module for the OpenSSH module. The files that make up the module are:

For x86_64

/usr/sbin/.sshd.hmac
/usr/sbin/sshd
/usr/share/man/man8/sshd.8.gz

/lib64/.libcrypto.so.0.9.8e.hmac
/lib64/.libcrypto.so.6.hmac
/lib64/.libssl.so.0.9.8e.hmac
/lib64/.libssl.so.6.hmac
/lib64/libcrypto.so.0.9.8e
/lib64/libcrypto.so.6
/lib64/libssl.so.0.9.8e
/lib64/libssl.so.6

/usr/bin/.fipscheck.hmac
/usr/bin/fipscheck

For IA64

/usr/sbin/.sshd.hmac
/usr/sbin/sshd
/usr/share/man/man8/sshd.8.gz

/lib/.libcrypto.so.0.9.8e.hmac
/lib/.libcrypto.so.6.hmac
/lib/.libssl.so.0.9.8e.hmac
/lib/.libssl.so.6.hmac
/lib/libcrypto.so.0.9.8e
/lib/libcrypto.so.6
/lib/libssl.so.0.9.8e
/lib/libssl.so.6

/usr/bin/.fipscheck.hmac
/usr/bin/fipscheck

The following table shows the overview of the security level for each of the eleven sections of the validation.

Security Component	Security Level
Cryptographic Module Specification	1
Cryptographic Module Ports and Interfaces	1
Roles, Services and Authentication	1
Finite State Model	1
Physical Security	N/A
Operational Environment	1
Cryptographic Key Management	1
EMI/EMC	1
Self Tests	1
Design Assurance	1
Mitigation of Other Attacks	N/A

Table 1, Security Levels

The module has been tested on the following multi-chip standalone platforms:

Manufacturer	Model	O/S & Ver.
HP	HP Integrity Server RX2660	Red Hat Enterprise Linux 5 (Single User Mode)
HP	HP ProLiant Server DL585	Red Hat Enterprise Linux 5 (Single User Mode)

Table 2, Tested Platforms

1.2 Description of Approved Mode

When in FIPS 140-2 approved mode, the contents of the file /proc/sys/crypto/fips_enabled will be '1'.

In Approved mode the module will support the following Approved functions/protocols:

- Triple-DES (Certs. #839, #840 and #841)
- AES (Certs. #1160, #1161 and #1162)
- DSA (Certs. #378, #379 and #380)
- RNG (ANSI X9.31) (Certs. #642, #643 and #644)
- HMAC-SHA1, HMAC-SHA256 (Certs. #661, #662 and #663)
- RSA (Certs. #549, #550 and #552)

The module will support the following Non-Approved functions (see caveat below)

- Diffie-Hellman (see caveat below)
- RSA (encrypt, decrypt) (see caveat below)

Note: The Red Hat Enterprise Linux 5 OpenSSH Server Cryptographic Module will use the Red Hat Enterprise Linux OpenSSL (FIPS 140-2 Validation #1320) Cryptographic Module for standard cryptographic operations and will require that a copy of a FIPS 140-2 level 1 validated version of the Red Hat Enterprise Linux OpenSSL

Cryptographic Module be installed on the system for the Red Hat Enterprise Linux 5 OpenSSH Server Cryptographic Module to operate in a validated mode.

The Red Hat Enterprise Linux 5 OpenSSH Server Cryptographic Module itself implements the SSHv2 protocol.

The module integrity check is performed by the Red Hat Enterprise Linux OpenSSL Cryptographic Module utility fipscheck. The version is 1.2.0-1.el5, and fipscheck-lib version is 1.2.0-1.el5 HMAC/SHA-256 (Certs #661, #862 and #663 from the Red Hat Enterprise Linux OpenSSL Cryptographic Module.)

CAVEAT:

The Module will support the following non-approved algorithms:

1) Diffie-Hellman will be used for key wrapping and establishment.(key agreement; key establishment methodology provides between 80 and 192 bits of encryption strength)

2) RSA (key wrapping; key establishment methodology provides between 80 and 150 bits of encryption strength)

1.3 Cryptographic Module Boundary

The physical module boundary is the surface of the case of the test platform. The logical module boundary is depicted in the software block diagram and is embodied by the SSH server application found at /usr/bin/sshd and the OpenSSL shared library module.

1.3.1 Hardware Block Diagram

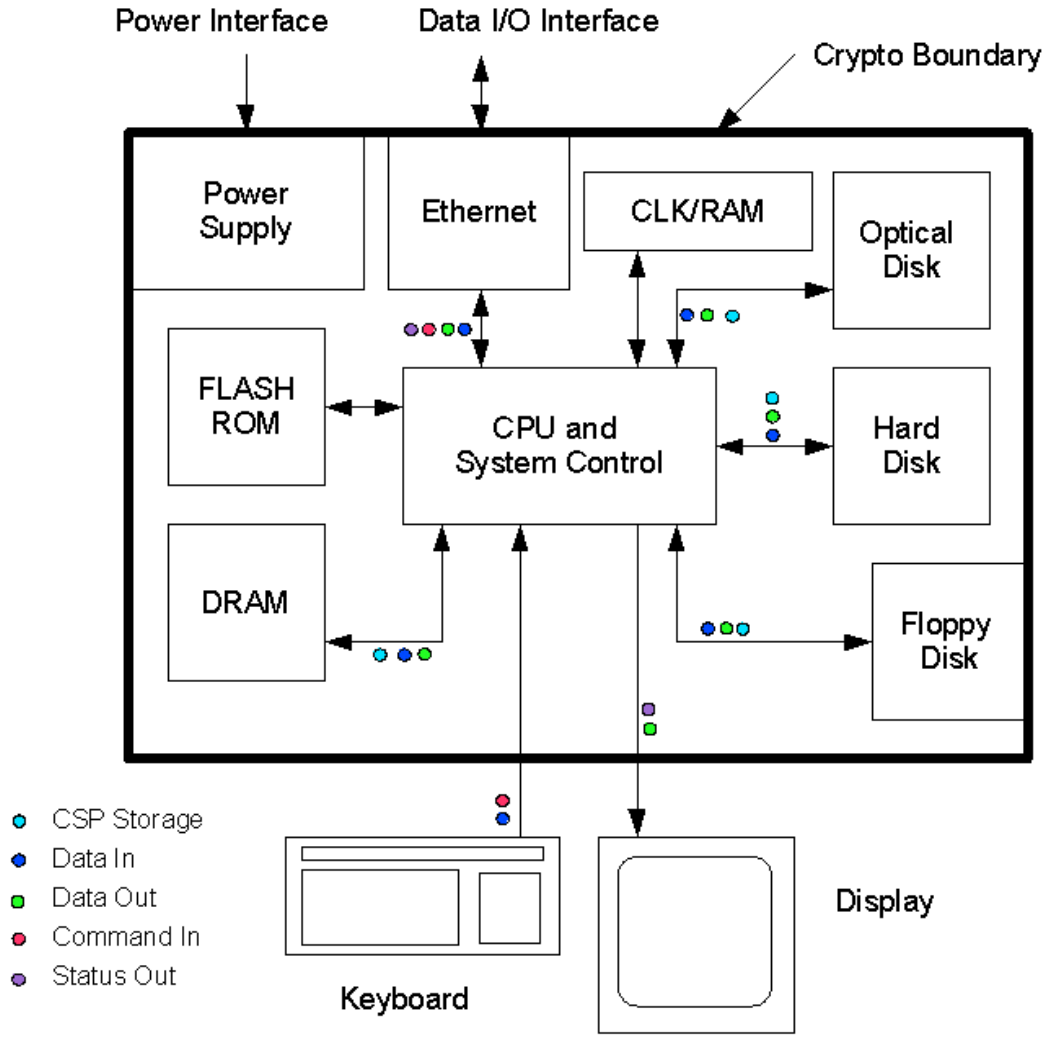

Figure 1, Hardware Block Diagram

1.3.2 Software Block Diagram

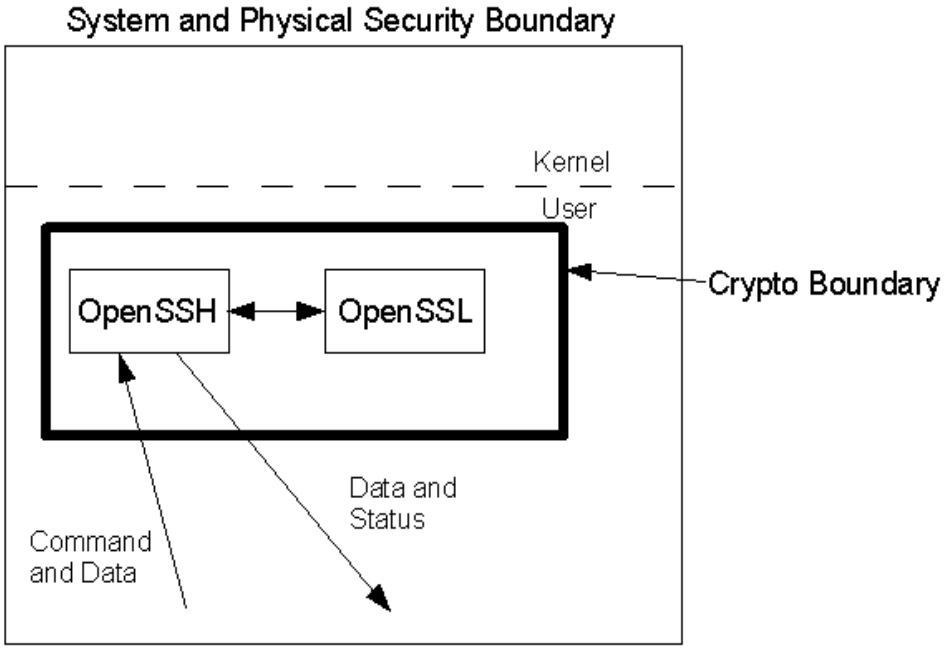

Figure 2, Software Block Diagram

2 Cryptographic Module Ports and Interfaces

Function	Port
Command In	Keyboard, Network, Configuration File /etc/ssh/sshd_config, Command Line Options
Status Out	Display, Network, System Log
Data In	Host Key Files in /etc/ssh, ~/.ssh/authorized_keys, Network
Data Out	Network, Virtual System Console

Table 3, Ports and Interfaces

3 Roles, Services and Authentication

This section defines the roles, services and authentication mechanisms and methods with respect to the applicable FIPS 140-2 requirements.

3.1 Roles

Role	Services (see list below)
User	Establish & Maintain SSH Session Close SSH Session (Zeroize) Show Status
Crypto Officer	Configure SSH Server Establish & Maintain SSH Session Close SSH Session (Zeroize) Terminate SSH Application Self-Tests Show Status

Table 4, Roles

3.2 Services

The module supports services that are available to users in the various roles. All of the services are described in detail in the module's user documentation. The following table shows the services available to the various roles and the access to cryptographic keys and CSPs resulting from services.

R – The item is read or referenced by the service.
W – The item is written or updated by the service.
Z – The persistent item is zeroized by the service.

All of the ciphers are from the Red Hat Enterprise Linux OpenSSL Cryptographic Module validated cryptographic module. The Red Hat Enterprise Linux 5 OpenSSH Server Cryptographic Module performs SSH v2 functions only, and passes all cryptographic operations to Red Hat Enterprise Linux OpenSSL Cryptographic Module.

Service	Category	Function	Role	Cryptographic Keys and CSPs Accessed	Access Type (RWZ)
Establish & Maintain SSH Session	Triple-DES	Encrypt/Decrypt, Keyed-Hash, Key Exchange, Sign/Verify	User, Crypto officer	RSA or DSA Server private key/public key Client Public Key DH private and public parameters, Session Encryption and Data Authentication Key s DRNG Seed and Seed Key	RWZ RW RW RW
Close SSH Session	None	Zeroize	User, Crypto officer	DH private and public parameters, Session	Z

Service	Category	Function	Role	Cryptographic Keys and CSPs Accessed	Access Type (RWZ)
				Encryption and Data Authentication Keys DRNG Seed and Seed Key	
Terminate SSH Application	None	Zeroize	Crypto officer	DH private and public parameters, Session Encryption and Data Authentication Keys DRNG Seed and Seed Key	Z
Self-Tests	Self Test (includes Integrity and known answer tests)	Invoked by restarting the module	Crypto officer	Software Integrity Key	R
Show Status	Status	Via verbose mode and exit codes	User, Crypto officer	None	N/A

Table 5, Services

3.3 Operator Authentication

There is no operator authentication, the role is implicit by action.

3.4 Mechanism and Strength of Authentication

No authentication is required at security level 1, authentication is implicit by assumption of the role.

4 Physical Security

This is a level one software module with no physical security.

5 Operational Environment

This module will operate in a modifiable operational environment per the FIPS 140-2 definition.

5.1 Policies

The operating system shall be restricted to a single operator mode of operation (i.e., concurrent operators are

explicitly excluded).

The operator that makes use of the cryptographic module is the single user.

In the FIPS approved mode the ptrace(2) system call, the debugger (gdb(1)) and strace(1) shall not be used.

6 Cryptographic Key Management

The following table identifies the Cryptographic Keys and Critical Security Parameters (CSPs) used within the module. Cryptographic keys and CSPs are never output from the module in plaintext. An Approved key generation method is used to generate keys that are generated by the module via OpenSSL.

6.1 Key life cycle table

Key	Type	Generation	Establishment	Access by Service	Entry and output method	Storage	Zeroization
Server Private Keys	DSA or RSA keys	N/A	N/A	Establish & Maintain SSH Session	N/A	Plaintext	Immediately after use
Server Public Keys (not a CSP)	DSA or RSA keys	N/A	N/A	Establish & Maintain SSH Session	Exported	Plaintext	N/A
Client Public Key	DSA or RSA key	N/A	N/A	Establish & Maintain SSH Session	Imported	Plaintext	N/A
Session Data Authentication Keys	HMAC SHA-1	N/A	Established during the SSH handshake through DH.	Establish & Maintain SSH Session	N/A	Ephemeral	Close SSH Session or Terminate SSH Application
Session Encryption Keys	AES or Triple-DES	N/A	Established during the SSH handshake through DH.	Establish & Maintain SSH Session	N/A	Ephemeral	Close SSH Session or Terminate SSH Application
Software Integrity Key	HMAC SHA-256	N/A	N/A	Self-Tests	N/A	Plaintext within the OpenSSL and fipscheck libraries	Terminate fipscheck Application
Diffie-Hellman Private and Public Parameters	DH	ANSI X9.31 RNG	N/A	Establish & Maintain SSH Session	N/A	Ephemeral	Close SSH Session or Terminate SSH Application

Key	Type	Generation	Establishment	Access by Service	Entry and output method	Storage	Zeroization
DRNG Seed	128-bit value	N/A	N/A	Establish & Maintain SSH Session	N/A, provided by /dev/urandom	Ephemeral	N/A (Termination of the SSH application where OpenSSL zeroizes seed)
DRNG Seed Key	128-bit value	N/A	N/A	Establish & Maintain SSH Session	N/A, provided / dev/urandom	Ephemeral	N/A (Termination of the SSH application where OpenSSL zeroizes key)

Table 6, Key Life Cycle

Notes:

The module ships without containing any keys and CSPs. When the module is configured, the Crypto officer can prevent a man-in-the-middle attack by confirming the user key is correct before storing the key in the .ssh/authorized_keys. Users may also perform this operation only on keys stored in their home directory.

The only key management operations during initial configuration include generating the server public-private key pair.

Diffie-Hellman key agreement transpires at the beginning of a session and with sessions after each 1 GB of data transfer or 1 hour of operation, whichever occurs first.

Persistently stored secret and private keys are out of scope, but may be zeroized using the a FIPS140-2 approved mechanism to clear data on hard disks.

6.2 Key Zeroization

For volatile memory, memset is included in deallocation operations. There are no restrictions when zeroizing any cryptographic keys and CSPs.

6.3 Random Number Generation

A FIPS 140-2, ANSI X9.31 approved pseudo random number generation mechanism will be used in the module, called from OpenSSL, which is seeded by the kernel.

The Linux kernel provides /dev/urandom as a source of random numbers for RNG seeds. The Linux kernel initializes this pseudo device at system startup.

The kernel performs continual tests on the random numbers it uses to ensure that the seed and seed key input to the Approved RNG do not have the same value. The kernel also performs continual tests on the output of the approved RNG to ensure that consecutive random numbers do not repeat.

7 Electromagnetic Interference/Electromagnetic Compatibility

Product Name and Model: HP ProLiant Server DL585 Series
Regulatory Model Number: HSTNS-1025
Product Options: All
conforms to the following Product Specifications and Regulations:
EMC: Class A
CISPR 22:2005
EN 55022:2006
EN 55024:1998 +A1:2001 +A2:2003
EN 61000-3-2:2006
EN 61000-3-3:1995 +A1:2001 +A2:2005

Product Name and Model: HP Integrity Server rx2660
Regulatory Model Number: RSVLA-0503
Product Options: All
conforms to the following Product Specifications and Regulations :
EMC: Class A
CISPR22:1997 / EN 55022:1998
CISPR 24:1997 + A1:2001 + A2: 2002 / EN 55024:1998 + A1:2001 + A2:2003
EN 61000-3-2:2000
EN 61000-3-3:1995 +A1:2001

8 Self Tests

FIPS 140-2 requires that the module perform self tests to ensure the integrity of the module and the correctness of the cryptographic functionality at start up. In addition some functions require continuous verification of function, such as the random number generator. All of these tests are listed and described in this section.

8.1 Power-Up Tests

Software Integrity Test. All cryptographic function tests are performed by the Red Hat Enterprise Linux OpenSSL module before it will perform cryptographic operations for the OpenSSH Server module.

8.1.1 Software Integrity Test Details

OpenSSH userspace modules have their integrity verified at startup by the software integrity test.

The integrity check is performed by the Red Hat Enterprise Linux OpenSSL module utility fipscheck. The version is 1.2.0-1.el5, and fipscheck-lib version is 1.2.0-1.el5 HMAC/SHA-256.

When the module starts, it exercises the power-on self-test including the software integrity test. The software integrity test (HMAC-SHA256) constitutes a known answer test for the HMAC-SHA256 algorithm.

The user space integrity verification is performed as follows:

> The OpenSSH server application links with the library libfipscheck.so which is intended to execute fipscheck to verify the integrity of the calling application file using HMAC SHA-256. Upon calling the FIPSCHECK_verify() function provided with libfipscheck.so, the fipscheck application is loaded and executed, and the following steps are performed.
>
> - OpenSSL as loaded by fipscheck performs the integrity check of the OpenSSL library files using HMAC SHA-256.
> - The application fipscheck performs the integrity check of its application file using HMAC SHA-256 provided by OpenSSL.

- The fipscheck application performs the integrity check of the calling application. The fipscheck computes the HMAC-SHA-256 checksum of the file from the command line and compares the computed value to the value stored inside the /path/to/application/.<applicationfilename>.hmac checksum file. The fipscheck application returns the appropriate exit value based on the comparison result (zero if the checksum is OK – which is enforced by the libfipscheck.so library).

9 Guidance

NOTE: All cryptographic functions for the Red Hat Enterprise Linux 5 OpenSSH Server Cryptographic Module will be provided by a copy of a FIPS 140-2 validated version of the Red Hat Open SSL cryptographic module.

9.1 Crypto officer and User Guidance

The version of the RPM containing the validated module is stated in section 1 above. The integrity of the RPM is automatically verified during the installation and the Crypto officer shall not install the RPM file if the RPM tool indicates an integrity error.

The RPM package of the module can be installed by standard tools recommended for the installation of RPM packages on a Red Hat Enterprise Linux system (for example, yum, rpm, and the RHN remote management tool).

For proper operation of the in-module integrity verification, the prelink has to be disabled. This can be done by setting PRELINKING=no in the /etc/sysconfig/prelink configuration file.

To bring the module into FIPS mode, the crypto officer has to regenerate the initrd by using the following command:

For the x86_64 platform, the command is:

```
mkinitrd --with-fips -f /boot/initrd-$(uname -r).img $(uname -r)
```

For the IA64, the command is:

```
mkinitrd --with-fips -f /boot/efi/efi/redhat/initrd-$(uname -r).img $(uname -r)
```

After regenerating the initrd, the crypto officer has to append the following string to the kernel command line by changing the setting in the boot loader:

```
fips=1
```

In addition to the configuration of the kernel, the OpenSSH server configuration file /etc/ssh/sshd_config should contain:

- Either no "Ciphers" option or the option with a subset out of "aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,3des-cbc,aes192-cbc,aes256-cbc";
- Either no "MACs" option or the option with "hmac-sha1";
- "Protocol 2" must be specified.

10 Glossary and Abbreviations

AES	Advanced Encryption Specification
CAVP	Cryptographic Algorithm Validation Program
CBC	Cypher Block Chaining
CCM	Counter with Cipher Block Chaining-Message Authentication Code
CFB	Cypher Feedback
CMT	Cryptographic Module Testing
CMVP	Cryptographic Module Validation Program
CSP	Critical Security Parameter
CVT	Component Verification Testing
DES	Data Encryption Standard
DH	Diffie-Hellman
DSA	Digital Signature Algorithm
ECB	Electronic Code Book
FSM	Finite State Model
HMAC	Hash Message Authentication Code
LDAP	Lightweight Directory Application Protocol
MAC	Message Authentication Code
NIST	National Institute of Science and Technology
NVLAP	National Voluntary Laboratory Accreditation Program
OFB	Output Feedback
O/S	Operating System
PRNG	Pseudo Random Number Generator
RNG	Random Number Generator
RSA	Rivest, Shamir, Addleman
SAP	Service Access Points
SDK	Software Development Kit
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SOF	Strength of Function
SSH	Secure Shell
TDES	Triple DES
UI	User Interface

Table 7, Abbreviations

11 References

[1] OpenSSH Server user guide (provided with installation RPM, see section 1.1 Description of Module for version)
[2] rx2660_EMIEMC_cert.pdf (On file at Red Hat)

[3] DL585_EMIEMC_CEcert.pdf (On file at Red Hat)

[4] FIPS 140-2 Standard, http://csrc.nist.gov/groups/STM/cmvp/standards.html

[5] FIPS 140-2 Implementation Guidance, http://csrc.nist.gov/groups/STM/cmvp/standards.html

[6] FIPS 140-2 Derived Test Requirements,http://csrc.nist.gov/groups/STM/cmvp/standards.html

[7] FIPS 197 Advanced Encryption Standard, http://csrc.nist.gov/publications/PubsFIPS.html

[8] FIPS 180-3 Secure Hash Standard, http://csrc.nist.gov/publications/PubsFIPS.html

[9] FIPS 198-1 The Keyed-Hash Message Authentication Code (HMAC), http://csrc.nist.gov/publications/PubsFIPS.html

[10] FIPS 186-3 Digital Signature Standard (DSS), http://csrc.nist.gov/publications/PubsFIPS.html

[11] ANSI X9.52:1998 Triple Data Encryption Algorithm Modes of Operation, http://webstore.ansi.org/FindStandards.aspx?Action=displaydept&DeptID=80&Acro=X9&DpName=X9,%20Inc.

