ORACLE®

LINUX

FIPS 140-2 Non-Proprietary Security Policy

Oracle Linux 6 OpenSSH Server Cryptographic Module

FIPS 140-2 Level 1 Validation

Software Version: R6-1.0.0

Date: September 28, 2017

Title: Oracle Linux 6 OpenSSH Server Cryptographic Module Security Policy

September 28, 2017

Author: Atsec Information Security

Contributing Authors:

Oracle Linux Engineering

Oracle Security Evaluations – Global Product Security

Oracle Corporation

World Headquarters

500 Oracle Parkway

Redwood Shores, CA 94065

U.S.A.

Worldwide Inquiries:

Phone: +1.650.506.7000

Fax: +1.650.506.7200

oracle.com

Hardware and Software, Engineered to Work Together

TABLE OF CONTENTS

List of Tables

List of Figures

1. Introduction

1.1 Overview

This document is the Security Policy for the Oracle Linux 6 OpenSSH Server Cryptographic Module by Oracle Corporation. Oracle Linux 6 OpenSSH Server Cryptographic Module is also referred to as "the Module" or "Module". This Security Policy specifies the security rules under which the module shall operate to meet the requirements of FIPS 140-2 Level 1. It also describes how the Oracle Linux 6 OpenSSH Server Cryptographic Module functions in order to meet the FIPS 140-2 requirements, and the actions that operators must take to maintain the security of the module.

This Security Policy describes the features and design of the Oracle Linux 6 OpenSSH Server Cryptographic Module using the terminology contained in the FIPS 140-2 specification. FIPS 140-2, Security Requirements for Cryptographic Module specifies the security requirements that will be satisfied by a cryptographic module utilized within a security system protecting sensitive but unclassified information. The NIST/CSE Cryptographic Module Validation Program (CMVP) validates cryptographic module to FIPS 140-2. Validated products are accepted by the Federal agencies of both the USA and Canada for the protection of sensitive or designated information.

1.2 Platforms

The validation was performed on a 64-bit system. According to FIPS 140-2 IG G.5, the CMVP allows vendor porting and recompilation of a validated module to similar platforms without involving code changes. Although the vendor may affirm the correct operation of the ported module on other platforms, the CMVP makes no statement as to the correct operation of the module or the security strengths of the generated keys when so ported.

1.3 Document Organization

The FIPS 140-2 Submission Package contains:

- Oracle Linux 6 OpenSSH Server Cryptographic Module Non-Proprietary Security Policy
- Other supporting documentation as additional references

With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Validation Documentation is proprietary to Oracle and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Oracle.

2. Oracle Linux 6 OpenSSH Server Cryptographic Module

2.1 Functional Overview

The Oracle Linux 6 OpenSSH Server Cryptographic Module (hereafter referred to as "the Module") is a software module implementing the cryptographic support for the SSH protocol in the Oracle Linux user space.

The Oracle Linux 6 OpenSSH Server Cryptographic Module is distributed with Oracle Linux open-source distributions. The Module implements SSH protocol and acts as a server daemon providing SSH service.

2.2 FIPS 140-2 Validation Scope

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

Security Requirements Section	Level
Cryptographic Module Specification	1
Cryptographic Module Ports and Interfaces	1
Roles and Services and Authentication	1
Finite State Machine Model	1
Physical Security	N/A
Operational Environment	1
Cryptographic Key Management	1
EMI/EMC	1
Self-Tests	1
Design Assurance	3
Mitigation of Other Attacks	N/A

Table 1: FIPS 140-2 Security Requirements

3. Cryptographic Module Specification

3.1 Definition of the Cryptographic Module

The Oracle Linux 6 OpenSSH Server Cryptographic Module is defined as software-only multi-chip standalone module as defined by the requirements within FIPS PUB 140-2. The logical cryptographic boundary of the module consists of the application, library files and their integrity check HMAC files, which are delivered through the Yum Package Manager (RPM) as listed below:

The module will use the Oracle Linux OpenSSL Cryptographic Module (FIPS 140-2 Certificate #3017) as a bound module which provides the underlying cryptographic algorithms necessary for establishing and maintaining the SSH session. In addition the integrity check uses the cryptographic services provided by the Oracle Linux OpenSSL Cryptographic Module as used by the utility application of fipscheck using the HMAC-SHA-256 algorithm.

This requires a copy of a Cert. #3017 validated version of the Oracle Linux OpenSSL Cryptographic Module to be installed on the system for the current module to operate.

The cryptographic Module combines a vertical stack of Oracle Linux components intended to limit the external interface each separate component may provide. The following software needs to be installed for the module to operate:

- Oracle Linux 6 OpenSSH Server Cryptographic Module with the version of the OpenSSH server RPM file openssh-5.3p1-122.el6.x86_64
- The bound module of OpenSSL with FIPS 140-2 Certificate #3017.
- The contents of the fipscheck RPM package (version 1.2.0-7.el6.x86_64)
- The contents of the fipscheck-lib RPM package (1.2.0-7.el6.x86_64).

The OpenSSH server RPM package of the Module includes the binary files, integrity check HMAC files and Man Pages. Any application other than the OpenSSH server application delivered with the aforementioned OpenSSH RPM packet is not part of the Module. The FIPS certificate for this module will not be valid if any other application than the OpenSSH server application is used.

The files comprising the module are the following:
- /usr/sbin/sshd
- /usr/sbin/.sshd.hmac
- /usr/bin/fipscheck
- /usr/bin/.fipscheck.hmac
- /lib64/libfipscheck.so.1.1.0
- /lib64/.libfipscheck.so.1.1.0.hmac

Figure 1 shows the logical block diagram of the module executing in memory on the host system.

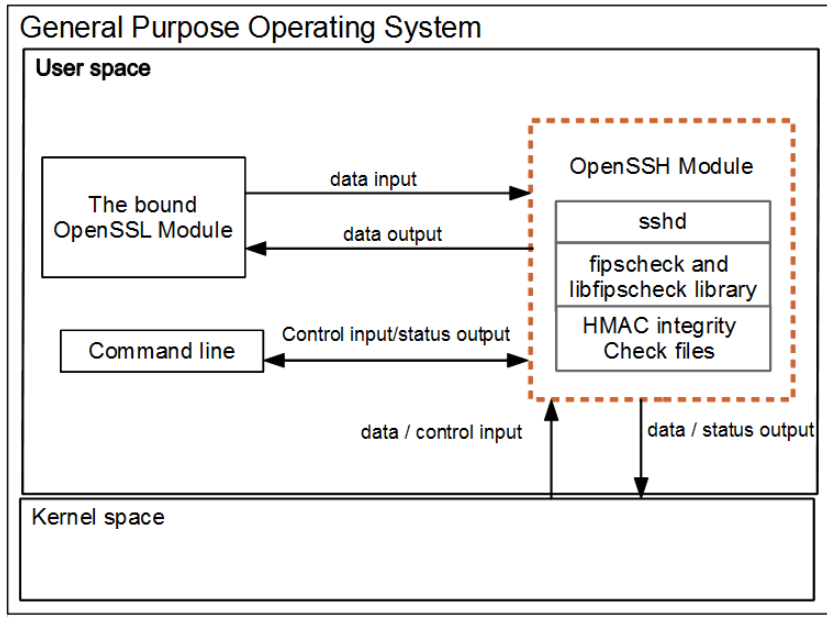**Figure 1: Oracle Linux 6 OpenSSH Server Logical Cryptographic Boundary**

3.2 Definition of the Physical Cryptographic Boundary

The physical cryptographic boundary is defined as the hard enclosure of the host system on which it runs. See Figure 2 below. No components are excluded from the requirements of FIPS PUB 140-2.
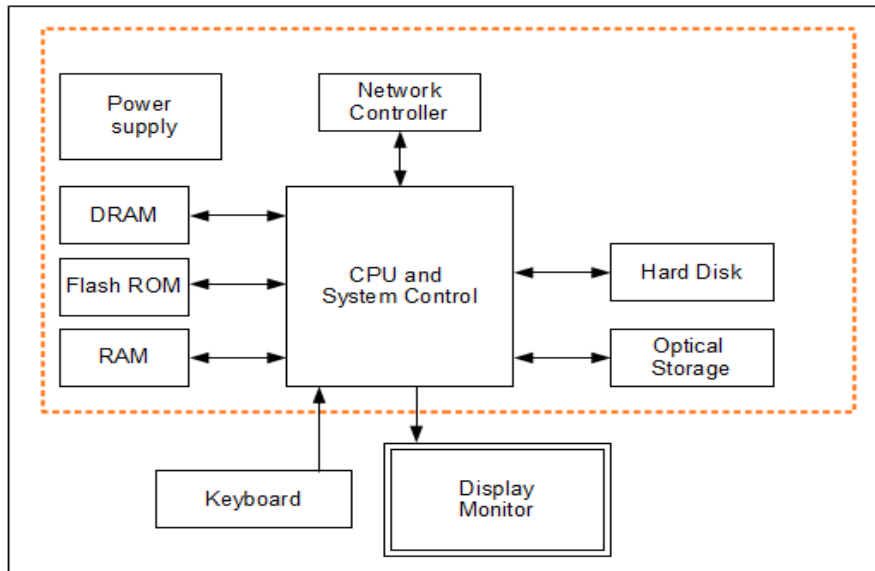
Figure 2: Oracle Linux 6 OpenSSH Server Hardware Block Diagram

3.3 Modes of Operation

The Module supports two modes of operation: FIPS approved and non-FIPS approved mode. The mode of operation is implicitly assumed depending on the services/security functions invoked. The Module turns to the FIPS approved mode after power-on self-tests succeed. The services available in FIPS mode can be found in section 7.2, Table 8.

3.4 Approved Security Function from OpenSSH module

The Oracle Linux 6 OpenSSH Server Cryptographic Module contains the following FIPS Approved Algorithms:

Approved or Allowed Security Functions		Certificate
Key Derivation (NIST SP 800-135 Section 5.2 for SSH)	(SHA 1, 256, 384, 512)	CVL #1254

Table 2: FIPS Approved Security Functions from OpenSSH Module

Note: The SSH protocol except the SP 800-135 Key Derivation Function has not been reviewed or tested by the CAVP and CMVP.

The OpenSSH and the bound OpenSSL module together provide the Diffie Hellman and EC Diffie Hellman key agreement. The OpenSSH module only implements the KDF portion of the key agreement as stated in the above table and the bound OpenSSL module provides the shared secret computation as stated in the below table.

- Diffie-Hellman (CVL Cert. #1216 with CVL cert. #1254, key agreement; key establishment methodology provides between 112 and 256 bits of encryption strength);
- EC Diffie-Hellman (CVL Cert. #1216 with CVL cert. #1254, key agreement; key establishment methodology provides between 112 and 256 bits of encryption strength);

3.5 Approved or Allowed Security Functions from the bound OpenSSL Module

The following are Approved or allowed security functions provided by the bound OpenSSL module.

Algorithm	Certificate
AES (CBC, CTR)	4533, 4535, 4537
Triple-DES (CBC)	2414
HMAC (SHA-1, SHA-256, SHA-512)	2995, 2991[1], 2993[1]
Diffie Hellman all except KDF shared secret computation	CVL 1216
EC Diffie-Hellman all except KDF shared secret computation (P-256,384,521)	CVL 1216
RSA	2468
DRBG CTR	1490, 1492, 1494
SHA (1,256,512)	3718, 3714[1], 3716[1]
ECDSA (P-256,384,521)	1104
NDRNG	Used for seeding NIST SP 800-90A DRBG

Table 3: Approved or Allowed Security Functions from OpenSSL module

---

[1] The referenced certificate supports SHA-1 only.

3.6 Non-Approved Security Function from OpenSSH module

The use of following non-Approved services will put the module in non-approved mode of operation implicitly:

Algorithm	Usage
RSA Signature Generation	Using keys less than 2048
DSA Signature Generation	With 1024-bit key

Table 4: Non-Approved Functions From OpenSSL Module

4. Module Ports and Interfaces

The module interfaces can be categorized as follows:

- Data Input Interface
- Data Output Interface
- Control Input interface
- Status Output Interface

As a software-only module, the module does not have physical ports. For the purpose of the FIPS 140-2 validation, the physical ports are interpreted to be the physical ports of the hardware platform on which the module runs. Table below, shows the mapping of ports and interfaces as per FIPS 140-2 Standard.

FIPS 140 Interface	Physical Port	Module Interfaces
Data Input	Ethernet Ports, keyboard	Input parameters of the sshd command on the command line with host key files in /etc/ssh, ~/.ssh/authorized_keys, locally stored data, data via SSHv2 channel, data via local or remote port-forwarding port, input data sent to the bound OpenSSL module via its API parameters.
Data Output	Display, Ethernet Port	Output data returned by the sshd command, output data sent via the SSHv2 channel, output data sent via local or remote port-forwarding port, output data sent to the bound OpenSSL module via its API parameters.
Control Input	Keyboard, Ethernet port	Invocation of the sshd command on the command line or via the configuration file /etc/ssh/sshd_config, SSHv2 protocol message requests received from SSH client
Status Output	Ethernet Port, Display	Status messages returned after the command execution, status of processing SSHv2 protocol message requests
Power	PC power supply	N/A

Table 5: Mapping of FIPS 140 Logical Interfaces to Logical Ports

5. Physical Security

The Module is comprised of software only and thus does not claim any physical security.

6. Operational Environment

The module operates in a modifiable operational environment per FIPS 140-2 Security Level 1 specifications. The module runs on a commercially available general-purpose operating system executing on the hardware specified in sections 6.1 and 6.2.

6.1 Tested Environments

The Module was tested on the following environments with and without PAA i.e. AES-NI:

Operating Environment	Processor	Hardware
Oracle Linux 6.9 64 bit	1. Intel® Xeon® CPU E5-2699 v4	Oracle Server X6-2

Table 6: Tested Operating Environment

6.2 Vendor Affirmed Environments

The following platforms have not been tested as part of the FIPS 140-2 level 1 certification however Oracle "vendor affirms" that these platforms are equivalent to the tested and validated platforms. Additionally, Oracle affirms that the module will function the same way and provide the same security services on any of the systems listed below.

Operating Environment	Processor	Hardware
Oracle Linux 6.9 64-bit	Intel® Xeon® E5-2600 v3 & v4	Cisco UCS B200 M4
Oracle Linux 6.9 64-bit	Intel® Xeon® E7-2800/E7-8800 v3	Cisco UCS B260 M4
Oracle Linux 6.9 64-bit	Intel® Xeon® E5-4600/E5-4600 v2	Cisco UCS B420 M3
Oracle Linux 6.9 64-bit	Intel® Xeon® E5-4600 v3 & v4	Cisco UCS B420 M4
Oracle Linux 6.9 64-bit	Intel® Xeon® E7-2800 v2/E7-4800 v2/E7-8800 v2/E7-4800 v3/E7-8800 v3	Cisco UCS B460 M4
Oracle Linux 6.9 64-bit	Intel® Xeon® E5-2400/E5-2400 v2	Cisco UCS C22 M3
Oracle Linux 6.9 64-bit	Intel® Xeon® E5-2600/E5-2600 v2	Cisco UCS C220 M3
Oracle Linux 6.9 64-bit	Intel® Xeon® E5-2600 v3 & v4	Cisco UCS C220 M4
Oracle Linux 6.9 64-bit	Intel® Xeon® E5-2400/E5-2400 v2	Cisco UCS C24 M3
Oracle Linux 6.9 64-bit	Intel® Xeon® E5-2600/E5-2600 v2	Cisco UCS C240 M3
Oracle Linux 6.9 64-bit	Intel® Xeon® E5-2600 v3 & v4	Cisco UCS C240 M4
Oracle Linux 6.9 64-bit	Intel® Xeon® E7-2800 v2/E7-4800 v2, v3 & v4/E7-8800 v2 & v4	Cisco UCS C460 M4
Oracle Linux 6.9 64-bit	Intel® Xeon® E5-2600 v3	Dell PowerEdge FC630
Oracle Linux 6.9 64-bit	Intel® Xeon® E5-4600 v3	Dell PowerEdge FC830
Oracle Linux 6.9 64-bit	Intel® Xeon® E5-2600 v3	Dell PowerEdge M630 Blade
Oracle Linux 6.9 64-bit	Intel® Xeon® E5-4600 v4	Dell PowerEdge M830 Blade
Oracle Linux 6.9 64-bit	Intel® Xeon® E5-2600 v3	Dell PowerEdge R630
Oracle Linux 6.9 64-bit	Intel® Xeon® E5-2600 v3	Dell PowerEdge R730
Oracle Linux 6.9 64-bit	Intel® Xeon® E5-2600 v3	Dell PowerEdge R730xd
Oracle Linux 6.9 64-bit	Intel® Xeon® E7-4800 v4	Dell PowerEdge R930
Oracle Linux 6.9 64-bit	Intel® Xeon® E5-2600 v3	Dell PowerEdge T630
Oracle Linux 6.9 64-bit	Intel® Xeon® E7-4800 v2/E7-8800 v2	Fujitsu PRIMEQUEST 2400E
Oracle Linux 6.9 64-bit	Intel® Xeon® E7-8800 v3	Fujitsu PRIMEQUEST 2400E2

Operating Environment	Processor	Hardware
Oracle Linux 6.9 64-bit	Intel® Xeon® E7-8800 v4	Fujitsu PRIMEQUEST 2400E3
Oracle Linux 6.9 64-bit	Intel® Xeon® E7-4800 v2	Fujitsu PRIMEQUEST2400L
Oracle Linux 6.9 64-bit	Intel® Xeon® E7-8800 v3	Fujitsu PRIMEQUEST2400L2
Oracle Linux 6.9 64-bit	Intel® Xeon® E7-8800 v4	Fujitsu PRIMEQUEST 2400L3
Oracle Linux 6.9 64-bit	Intel® Xeon® E7-4800 v2	Fujitsu PRIMEQUEST 2400S
Oracle Linux 6.9 64-bit	Intel® Xeon® E7-4800 v2	Fujitsu PRIMEQUEST 2400S Lite
Oracle Linux 6.9 64-bit	Intel® Xeon® E7-8800 v3	Fujitsu PRIMEQUEST 2400S2
Oracle Linux 6.9 64-bit	Intel® Xeon® E7-8800 v3	Fujitsu PRIMEQUEST 2400S2 Lite
Oracle Linux 6.9 64-bit	Intel® Xeon® E7-8800 v4	Fujitsu PRIMEQUEST 2400S3
Oracle Linux 6.9 64-bit	Intel® Xeon® E7-8800 v4	Fujitsu PRIMEQUEST 2400S3 Lite
Oracle Linux 6.9 64-bit	Intel® Xeon® E7-8800 v2	Fujitsu PRIMEQUEST 2800B
Oracle Linux 6.9 64-bit	Intel® Xeon® E7-8800 v3	Fujitsu PRIMEQUEST 2800B2
Oracle Linux 6.9 64-bit	Intel® Xeon® E7-8800 v4	Fujitsu PRIMEQUEST 2800B3
Oracle Linux 6.9 64-bit	Intel® Xeon® E7-8800 v2	Fujitsu PRIMEQUEST 2800E
Oracle Linux 6.9 64-bit	Intel® Xeon® E7-8800 v3	Fujitsu PRIMEQUEST 2800E2
Oracle Linux 6.9 64-bit	Intel® Xeon® E7-8800 v4	Fujitsu PRIMEQUEST 2800E3
Oracle Linux 6.9 64-bit	Intel® Xeon® E7-8800 v2	Fujitsu PRIMEQUEST 2800L
Oracle Linux 6.9 64-bit	Intel® Xeon® E7-8800 v3	Fujitsu PRIMEQUEST 2800L2
Oracle Linux 6.9 64-bit	Intel® Xeon® E7-8800 v4	Fujitsu PRIMEQEST 2800L3
Oracle Linux 6.9 64-bit	Intel® Xeon® E5-2600 v3	Fujitsu PRIMERGY BX2580 M1
Oracle Linux 6.9 64-bit	Intel® Xeon® E5-2600 v4	Fujitsu PRIMERGY BX2580 M2
Oracle Linux 6.9 64-bit	Intel® Xeon® E5-2600 v3	Fujitsu PRIMERGY RX2530 M1
Oracle Linux 6.9 64-bit	Intel® Xeon®E5-2600 v4	Fujitsu PRIMERGY RX2530 M2
Oracle Linux 6.9 64-bit	Intel® Xeon® E5-2600 v3	Fujitsu PRIMEGY RX2540 M1
Oracle Linux 6.9 64-bit	Intel® Xeon® E5-2600 v4	Fujitsu PRIMERGY RX2540 M2
Oracle Linux 6.9 64-bit	Intel® Xeon® E7-4800 v3/E7-8800 v3	Fujitsu PRIMERGY RX4770 M2
Oracle Linux 6.9 64-bit	Intel® Xeon® E7-4800 v4/E7-8800 v4	Fujitsu PRIMERGY RX4770 M3
Oracle Linux 6.9 64-bit	Intel® Xeon® E5-2600 v3	Hitachi BladeSymphony BS2500 HC0A1
Oracle Linux 6.9 64-bit	Intel® Xeon® E5-2600 v4	Hitachi BladeSymphony BS2500 HE0A2
Oracle Linux 6.9 64-bit	Intel® Xeon® E7-4800 v3/E7-8800 v3	Hitachi BladeSymphony BS2500 HE0E2
Oracle Linux 6.9 64-bit	Intel® Xeon®E5-2600 v3	Hitachi BladeSymphony BS500 BS520H B3
Oracle Linux 6.9 64-bit	Intel® Xeon® E7-4800 v3/E7-8800 v3	Hitachi BladeSymphony BS500 BS520X B2
Oracle Linux 6.9 64-bit	Intel® Xeon® E5-2600 v3	Hitachi Compute Blade 2500 CB520H B3
Oracle Linux 6.9 64-bit	Intel® Xeon® E5-2600 v4	Hitachi Compute Blade 2500 CB520H B4
Oracle Linux 6.9 64-bit	Intel® Xeon® E7-8800 v2	Hitachi Compute Blade 2500 CB520X B2
Oracle Linux 6.9 64-bit	Intel® Xeon® E7-8800 v3	Hitachi Compute Blade 2500 CB520X B3
Oracle Linux 6.9 64-bit	Intel® Xeon® E5-2600 v3	Hitachi Compute Blade 500 CB520H B3

Operating Environment	Processor	Hardware
Oracle Linux 6.9 64-bit	Intel® Xeon® E7-8800 v2	Hitachi Compute Blade 500 CB520X B2
Oracle Linux 6.9 64-bit	Intel® Xeon® E5-2600 v4	Hitachi HA8000 RS210 AN2
Oracle Linux 6.9 64-bit	Intel® Xeon® E5-2600 v4	Hitachi HA8000 RS220 AN2
Oracle Linux 6.9 64-bit	Intel® Xeon® E5-2600 v4	Hitachi QuantaGrid D51B-2U
Oracle Linux 6.9 64-bit	Intel® Xeon® E5-2600 v3 & v4	Hitachi QuantaPlex T41S-2U
Oracle Linux 6.9 64-bit	Intel® Xeon® E5-2600 v2	HPE ProLiant BL460c Gen8
Oracle Linux 6.9 64-bit	Intel® Xeon® E5-2600 v3	HPE ProLiant BL460c Gen9
Oracle Linux 6.9 64-bit	AMD Opteron 6300-series	HPE ProLiant BL465c Gen8
Oracle Linux 6.9 64-bit	Intel® Xeon® E5-4600 v2	HPE ProLiant BL660c Gen8
Oracle Linux 6.9 64-bit	Intel® Xeon® E5-4600 v3	HPE ProLiant BL660c Gen9
Oracle Linux 6.9 64-bit	Intel® Xeon® E5-2600 v3 & v4	HPE ProLiant DL120 Gen9
Oracle Linux 6.9 64-bit	Intel® Xeon® E5-2600 v3 & v4	HPE ProLiant DL180 Gen9
Oracle Linux 6.9 64-bit	Intel ® Pentium® G2120 & Intel® Xeon® E3-1200 v2	HPE ProLiant DL320e Gen8
Oracle Linux 6.9 64-bit	Intel® Pentium® G3200-series/G3420, Core i3-4100-series/Intel® Xeon® E3-12 v3	HPE ProLiant DL320e Gen8 v2
Oracle Linux 6.9 64-bit	Intel® Xeon® E5-2600 v3 & v4	HPE ProLiant DL360 Gen9
Oracle Linux 6.9 64-bit	Intel® Xeon® E5-2400/E5-2400 v2	HPE ProLiant DL360e Gen8
Oracle Linux 6.9 64-bit	Intel® Xeon® E5-2600 v3 & v4	HPE ProLiant DL360p Gen8
Oracle Linux 6.9 64-bit	Intel® Xeon® E5-2600 v3 & v4	HPE ProLiant DL380 Gen9
Oracle Linux 6.9 64-bit	Intel® Xeon® E5-2400/E5-2400 v2	HPE ProLiant DL380e Gen8
Oracle Linux 6.9 64-bit	Intel® Xeon® E5-2600/E5-2600 v2	HPE ProLiant DL380p Gen8
Oracle Linux 6.9 64-bit	Intel® Xeon®E5-4600 v3 & v4	HPE ProLiant DL560 Gen9
Oracle Linux 6.9 64-bit	Intel® Xeon® E7-4800 v2/E7-8800 v2	HPE ProLiant DL580 Gen8
Oracle Linux 6.9 64-bit	Intel® Xeon® E7-4800 v3/E7-8800 v3	HPE ProLiant DL580 Gen9
Oracle Linux 6.9 64-bit	Intel® Xeon® X7560, X6550, E6540, E7520	HPE ProLiant DL980 G7
Oracle Linux 6.9 64-bit	Intel® Xeon® E5-2600 v3 & v4	HPE ProLiant ML350 Gen9
Oracle Linux 6.9 64-bit	Intel® Xeon® E5-2600 v3	HPE ProLiant XL450 Gen9 (Apollo 4500)
Oracle Linux 6.9 64-bit	Intel® Xeon® E5-2600 v4	HPE Synergy 480 Gen9 Compute Module
Oracle Linux 6.9 64-bit	Intel® Xeon®E7-4800 v4/E7-8800 v4	HPE Synergy 620 Gen9 Compute Module
Oracle Linux 6.9 64-bit	Intel® Xeon® E7-4800 v4/E7-8800 v4	HPE Synergy 680 Gen9 Compute Module
Oracle Linux 6.9 64-bit	Intel® Xeon® E5-2600 v3	Inspur Yingxin NF5180M4
Oracle Linux 6.9 64-bit	Intel® Xeon® E5-2600 v3 & v4	Inspur Yingxin NF5240M4
Oracle Linux 6.9 64-bit	Intel® Xeon® E5-2600 v2	Inspur Yingxin NF5270M3
Oracle Linux 6.9 64-bit	Intel® Xeon® E5-2600 v3 & v4	Inspur Yingxin NF5280M4
Oracle Linux 6.9 64-bit	Intel® Xeon® E7-4800 v3 & v4/E7-8800 v3 & v4	Inspur Yingxin NX8480M4
Oracle Linux 6.9 64-bit	Intel® Xeon® E5-2600 v4	Lenovo System x3650 M5
Oracle Linux 6.9 64-bit	Intel® Xeon® E7-4800 v4/E7-8800 v4	Lenovo System x3850 X6
Oracle Linux 6.9 64-bit	Intel® Xeon® E5-4800 v4/E7-8800 v4	NEC Express 5800/R120g-1M
Oracle Linux 6.9 64-bit	Intel® Xeon® E5-2600 v4	NEC Express 5800/R120g-2M
Oracle Linux 6.9 64-bit	Intel® Xeon® E5-2600 v3	Oracle Netra Server X5-2

Operating Environment	Processor	Hardware
Oracle Linux 6.9 64-bit	Intel® Xeon® E5-2600 v3	Oracle Server X5-2
Oracle Linux 6.9 64-bit	Intel® Xeon® E5-2600 v4	Oracle Server X6-2L
Oracle Linux 6.9 64-bit	Intel® Xeon® E5-2600 v4	Oracle Server X6-2M
Oracle Linux 6.9 64-bit	Intel® Xeon® E5-2600	Oracle Sun Server X3-2
Oracle Linux 6.9 64-bit	Intel® Xeon® E5-2600	Oracle Sun Server X3-2L
Oracle Linux 6.9 64-bit	Intel® Xeon® E5-2600 v2	Oracle Sun Server X4-2
Oracle Linux 6.9 64-bit	Intel® Xeon® E5-2600 v2	Oracle Sun Server X4-2L

Table 7: Vendor Affirmed Operating Environment

CMVP makes no statement as to the correct operation of the module or the security strengths of the generated keys when so ported if the specific operational environment is not listed on the validation certificate.

6.3 Operational Environment Policy

The operating system is restricted to a single operator (concurrent operators are explicitly excluded). The entity using the application is the single user of the module. In FIPS Approved mode, the ptrace(2) system call, the debugger (gdb(1)), and strace(1) shall be not used.

7. Roles, Services and Authentication

7.1 Roles

The roles are implicitly assumed by the entity accessing the module services. The Module supports the following roles:

- **User Role**: Performs services to establish, maintain and close SSH session, show status and self-tests.
- **Crypto Officer Role**: Performs module installation and configuration and terminate sshd Application.

7.2 FIPS Approved Services and Descriptions

The following table shows the available services, the roles allowed, the Critical Security Parameters (CSPs) involved and how they are accessed in the FIPS mode. In the table below, the "U" represents a User Role, and "CO" denotes a Crypto Officer role.

U	CO	Service Name	Service Description	Keys and CSP(s)	Access Type(s)
X		Establish SSH Session	SSH authentication	RSA or ECDSA key pair	R, W, X
			Negotiate a SSH V2 key agreement	Diffie-Hellman or EC Diffie-Hellman key pair	
			Key derivation using SP800-135 SSH KDF	shared secret, derived session encryption keys (Triple-DES or AES), and derived data authentication (HMAC) keys	
X		Maintain SSH Session	Provide data encryption and data authentication over SSH V2 network protocol	Derived session encryption keys (Triple-DES or AES), and derived data authentication (HMAC) keys	R
X		Close SSH session	Zeroize SSH derived session encryption and data authentication keys by closing the SSH session	Derived session encryption key (Triple-DES or AES) and data authentication keys, shared secret	Z
	X	Terminate sshd application	Zeroize SSH derived session encryption and data authentication keys by terminating the sshd application		
X		Self-Test	Perform on-demand self-tests	None	R, X
X		Show Status	Show status of the module	None	R, X
	X	Installation	Install the SSH Server	None	X
	X	Configure SSH Server	Configure the SSH Server	None	R, W, X

R – Read, W – Write, X – Execute, Z – Zeroize

Table 8: FIPS Approved Services and Descriptions

7.3   Non FIPS Approved Services and Descriptions

The following table shows Non FIPS approved services. Any use of these services will put the module in non-FIPS mode implicitly.

U	CO	Service Name	Service Description	Keys and CSP(s)	Access Type(s)
X		Establish SSH Session	SSH authentication	RSA, DSA with keys listed in Table 4	R, W, X

Table 9: Non FIPS Approved Services and Descriptions

7.4   Operator Authentication

The module does not support operator authentication mechanisms.

8. Key and CSP Management

The following keys, cryptographic key components and other critical security parameters are contained in the module.

CSP Name	Generation/Input	Use	Zeroization
Shared Secret	N/A (entered via API parameter from the bound OpenSSL module)	Shared secrete used to derive session keys.	Zeroized by closing SSH session or terminating the the sshd application
Derived session key (AES, Triple-DES,HMAC)	N/A (derived from the shared secret via SP800-135 SSH KDF)	SSH session keys used for encrypt/decrypt and data authentication operations.	
Server RSA private Key	N/A (keys are read from the host key file)	RSA server private key used to authenticate SSH server	
Server ECDSA private Key		ECDSA private key used to authenticate SSH server	
Server EC Diffie-Hellman private Key	N/A (keys are entered from the bound OpenSSL Module via API parameters)	EC Diffie-Hellman private key used as part of the key agreement protocol.	
Server Diffie-Hellman private Key		Diffie-Hellman private key used as part of the key agreement protocol.	

Table 10: CSP Table

8.1 Random Number and Key Generation

The module does not implement any random number generator nor does it provides key generation. The module only provides key derivation through the implementation of the SP 800-135 KDF.

When establishing the SSH Session, the module calls the bound OpenSSL module which generates the shared secret. The module derives keys from this shared secret by applying SP 800-135 KDF. When the module requests encryption/decryption services provided by the OpenSSL bound module, the resulting derived symmetric key (i.e. the output of the SP 800-135 KDF) will be passed to the OpenSSL bound module via API parameters. The module does not support manual key entry.

8.2 Key/CSP Storage

The module does not perform persistent storage of keys. The keys and CSPs are temporarily stored as plaintext in the RAM. The server's public and private keys are stored in the host key files in /etc/ssh directory, which are outside its logical boundary.

8.3 Key/CSP Zeroization
The destruction functions overwrite the memory occupied by keys with zeros and deallocate the memory. In case of abnormal termination, or swap in/out of a physical memory page of a process, the keys in physical memory are overwritten before the physical memory is allocated to another process.

9. Self-Tests

9.1 Power-Up Self-Tests

The module performs power-up self-tests at module initialization to ensure that the module is not corrupted. The self-tests are automatically triggered without any user intervention.

While the module is performing the power-up tests, services are not available, and input or output data is not possible: the module is not available until the self-tests are completed successfully.

9.1.1 Integrity Tests

The integrity check is performed by the fipscheck application using the HMAC-SHA-256 algorithm implemented by the bound Oracle Linux OpenSSL Cryptographic Module. When the OpenSSH module starts, it triggers the power-on self-tests, which includes the software integrity test.

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 OpenSSH server application file using the HMAC-SHA-256 algorithm. Upon calling the FIPSCHECK_verify() function provided with libfipscheck.so, fipscheck is loaded and executed, and the following steps are performed:

1. OpenSSL, loaded by fipscheck, performs the integrity check of the OpenSSL library files using the HMAC-SHA-256 algorithm
2. fipscheck performs the integrity check of its application file using the HMAC-SHA-256 algorithm provided by the OpenSSL Module
3. fipscheck automatically verifies the integrity of libfipscheck.so before processing requests of calling applications
4. The fipscheck application performs the integrity check of the OpenSSH server application file. The fipscheck computes the HMAC-SHA-256 checksum of that and compares the computed value with the value stored inside the .sshd.hmac checksum file. The fipscheck application returns the appropriate exit value based on the comparison result: zero if the checksum is OK, an error code otherwise (which brings the OpenSSH Module into the error state). The libfipscheck.so library reports the result to the OpenSSH server application.

If any of those steps fail, an error code is returned and the OpenSSH Module enters the error state with the message 'FIPS integrity verification test failed'. In Error state, all data output is inhibited and no cryptographic operation is allowed. The module needs to be reloaded in order to recover from the Error state.

9.1.2 Cryptographic Algorithm Tests

The OpenSSH module will use the Oracle Linux OpenSSL Cryptographic Module as a bound module which provides the underlying cryptographic algorithms. All the known answer tests are implemented by the bound OpenSSL Module.

9.1.3 On-Demand Self-Tests

The module provides the Self-Test service to perform self-tests on demand. On demand self-tests can be invoked by powering-off and reloading the module. This service performs the same tests executed during power-up. During the execution of the on-demand self-tests, crypto services are not available and no data output or input is possible.

10. Crypto-Officer and User Guidance

The following guidance items are to be used for assistance in maintaining the module's validated status while in use.

10.1 Crypto-Officer Guidance

The version of the Oracle Package Manager containing the FIPS validated Module is stated in section 3.1 above. The Oracle Linux OpenSSL Cryptographic Module referenced in section 3.1 must be installed according to its Security Policy.

As stated in Guidance section of Oracle Linux OpenSSL Cryptographic Module security policy, after configuring the operating environment to support FIPS, the file /proc/sys/crypto/fips_enabled will contain 1. If the file does not exist or does not contain "1", the operating environment is not configured to support FIPS and the module will not operate as a FIPS validated module.

After performing the configuration, the Crypto Officer should proceed for module installation. The RPM package of the Module can be installed by standard tools recommended for the installation of Oracle packages on an Oracle Linux system (for example, yum, RPM, and the RHN remote management tool). The integrity of the RPM is automatically verified during the installation of the Module and the Crypto Officer shall not install the RPM file if the Oracle Linux Yum Server indicates an integrity error. The RPM files listed in section 3 are signed by Oracle and during installation; Yum performs signature verification which ensures as secure delivery of the cryptographic module. If the RPM packages are downloaded manually, then the CO should run 'rpm –K <rpm-file-name>' command after importing the builder's GPG key to verify the package signature. In addition, the CO can also verify the hash of the RPM package to confirm a proper download.

10.1.1 OpenSSH Server Configuration

The user must not use DSA keys for performing SSH authentication as OpenSSH only allows DSA keys with 1024 bit size which are disallowed as per SP800-131A.

The user must not accept DSA host keys potentially offered during the first contact of an SSH server as OpenSSH only allows DSA keys with 1024 bit size which are disallowed as per SP800- 131A.

When re-generating RSA host keys, the crypto officer should generate RSA keys with a size of 2048 bit or higher according to [SP800-131A]. The crypto officer should inform the user base to not use RSA keys with key sizes smaller than 2048 bits. Any use of non-Approved key size or algorithms will result in the module entering the non-FIPS mode of operation.

With operating environment setup as stated in the above section, the following restrictions are applicable. For the module, the mode of operation is implicitly assumed depending on the services/security functions invoked as stated in section 3.3 and the successive sections lists the available ciphers from the module. No more cipher addition is possible by configuration it can only choose form the available ciphers.

- SSH protocol version 1 is not allowed
- GSSAPI is not allowed
- Only the following ciphers are allowed:
  - aes128-ctr

- o aes192-ctr
- o aes256-ctr
- o aes128-cbc
- o aes192-cbc
- o aes256-cbc
- o 3des-cbc
- o rijndael-cbc@lysator.liu.se

Only the following message authentication codes are allowed:
- hmac-sha1
- hmac-sha2-256
- hmac-sha2-512

10.2 User Guidance

Use the 'service sshd start' command to start the OpenSSH server, or configure the server to start using 'chkconfig'. This module is used by connecting to it with a ssh client. See the documentation of the client, e.g. the Oracle Linux 6 OpenSSH Client Cryptographic Module's Security Policy and the sshd(1) man page, for more information.

10.2.1 Handling Self-Test Errors

The OpenSSH self-test consists of the software integrity test. If the integrity test fails, OpenSSH enters an error state. To recover from the error state, the module must be restarted. If the failure persists, the module must be reinstalled. The bound OpenSSL module's self-tests failures will prevent OpenSSH from operating. See the Guidance section in the OpenSSL Security Policy for instructions on handling OpenSSL self-test failures.

11. Mitigation of Other Attacks

The Oracle Linux 6 OpenSSH Server cryptographic module does not mitigate against attacks.

Acronyms, Terms and Abbreviations

Term	Definition
AES	Advanced Encryption Standard
CMVP	Cryptographic Module Validation Program
CSP	Critical Security Parameter
DRBG	Deterministic Random Bit Generator
ECDSA	Elliptic Curve Digital Signature Algorithm
HMAC	(Keyed) Hash Message Authentication Code
KDF	Key Derivation Function
NIST	National Institute of Standards and Technology
PAA	Processor Algorithm Acceleration
PUB	Publication
SHA	Secure Hash Algorithm
SSH	Secure Shell

Table 11: Acronyms

References

The FIPS 140-2 standard, and information on the CMVP, can be found at
http://csrc.nist.gov/groups/STM/cmvp/index.html. More information describing the module can be found on the
Oracle web site at www.oracle.com .

This Security Policy contains non-proprietary information. All other documentation submitted for FIPS 140-2
conformance testing and validation is "Oracle - Proprietary" and is releasable only under appropriate non-
disclosure agreements.

Document	Author	Title
FIPS PUB 140-2	NIST	FIPS PUB 140-2: Security Requirements for Cryptographic Modules
FIPS IG	NIST	Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program
NIST SP 800-135	NIST	Recommendation for Existing Application-Specific Key Derivation Functions
NIST SP 800-131A	NIST	Recommendation for the Transitioning of Cryptographic Algorithms and Key Sizes

Table 12: References