ORACLE®
Linux

FIPS 140-2 Non-Proprietary Security Policy

Oracle Linux 6 Kernel Crypto API Cryptographic Module

FIPS 140-2 Level 1 Validation

Software Version: R6-1.0.0

Date: March 06, 2019

©Oracle Corporation

This document may be reproduced whole and intact including the Copyright notice.

Title: Oracle Linux 6 Kernel Crypto API Cryptographic Module Security Policy
Date: March 06, 2019
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


Oracle is committed to developing practices and products that help protect the environment

Copyright © 2019, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. Oracle specifically disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. This document may reproduced or distributed whole and intact including this copyright notice.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Hardware and Software, Engineered to Work Together

ORACLE

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 Kernel Crypto API Cryptographic Module by Oracle Corporation. Oracle Linux 6 Kernel Crypto API 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 Kernel Crypto API Cryptographic Module functions in order to meet the FIPS 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 Kernel Crypto API 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 Document Organization

The Submission Package contains:

- Oracle Linux 6 Kernel Crypto API 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 Kernel Crypto API Cryptographic Module

2.1 Functional Overview

The Oracle Linux 6 Kernel Crypto API Cryptographic Module (hereafter referred to as the "Module") is a software only cryptographic module that provides general-purpose cryptographic services to the remainder of the Linux kernel. The Oracle Linux 6 Kernel Crypto API Cryptographic Module is software only, security level 1 cryptographic module, running on a multi-chip standalone platform.

2.2 FIPS 140-2 Validation Scope

The following table shows the security level for each of the eleven sections of the validation. See Table 1 below.

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 Kernel Crypto API is defined as a multi-chip standalone module as defined by the requirements within FIPS PUB 140-2. The logical cryptographic boundary of the module consists of shared library files and their integrity check HMAC files, which are delivered through the Oracle Public Yum Package Manager (RPM) as listed below:

The list of components required for the module to operate are defined below:

- Oracle Linux 6 Kernel Crypto API Cryptographic Module with the version of the RPM file kernel-2.6.32-754.3.5.0.1.el6.x86_64.rpm
- The configuration of the FIPS mode is provided by the dracut-fips and dracut-fips-aesni package with the version of the RPM file of 004-409.0.8.el6_8.2.x86_64
- The bound module Oracle Linux NSS Cryptographic Library with FIPS 140-2 Certificate #3111 (hereafter referred to as the "NSS bound module" or "NSS module")
- The contents of the hmaccalc RPM package 0.9.12-2.el6.x86_64

The Oracle Linux 6 Kernel Crypto API RPM package of the Module includes the binary files, integrity check HMAC files and Man Pages. The files comprising the module are the following:

- kernel object files /lib/modules/$(uname -r)/kernel/crypto/*.ko
- kernel object files /lib/modules/$(uname -r)/kernel/arch/x86/crypto/*.ko
- static kernel binary /boot/vmlinuz-$(uname -r)
- static kernel binary HMAC file /boot/.vmlinuz-$(uname -r).hmac
- sha512hmac binary file for performing the integrity checks /usr/bin/sha512hmac
- sha512hmac binary HMAC file: /usr/lib64/hmaccalc/sha512hmac.hmac

The NSS bound module provides the HMAC-SHA-512 algorithm used by the sha512hmac binary file to verify the integrity of both the sha512hmac file and the vmlinuz (static kernel binary).

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

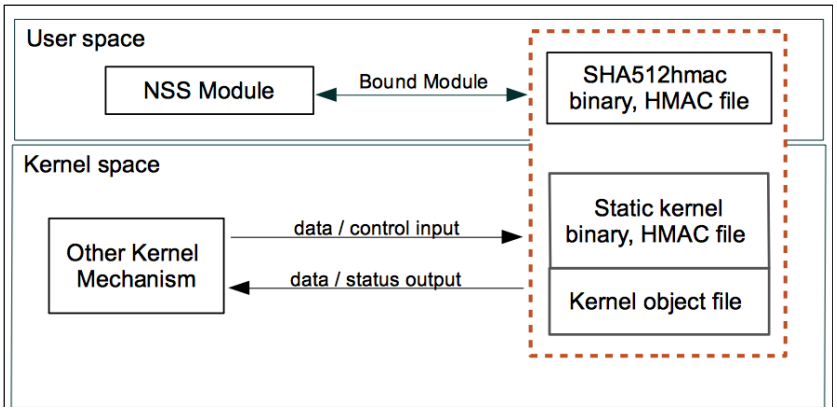

Figure 1: Oracle Linux 6 Kernel Crypto API Logical Cryptographic Boundary

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.

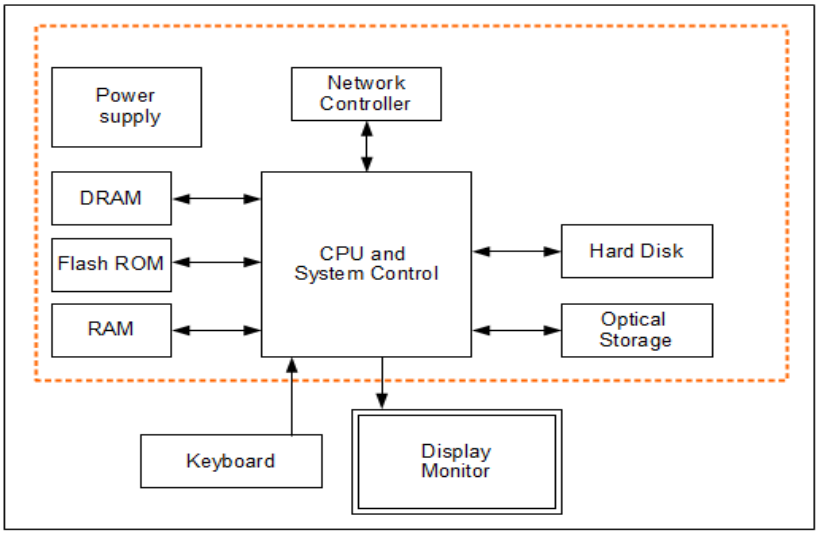

Figure 2: Oracle Linux 6 Kernel Crypto API Hardware Block Diagram

3.3 Modes of Operation

The module supports two modes of operation: the FIPS approved and non-approved modes.

Section 10.1.1 describes the Secure Installation and Startup to correctly install and configure the module. The module turns to FIPS approved mode after correct initialization, successful completion of power-on self-tests.

Invoking a non-Approved algorithm or a non-Approved key size with an Approved algorithm as listed in Table 4 will result in the module implicitly entering the non-FIPS mode of operation. After completion of the service the module will implicitly transition back to the FIPS mode and then depending on the next service call it will either remain in FIPS mode or will transition to non-approved mode.

The approved services available in FIPS mode can be found in section 7.2, Table 8**.** The non-approved services available in non-FIPS mode can be found in section 7, **Table 9**.

3.4 Approved or Allowed Security Functions

The Oracle Linux 6 Kernel Crypto API Cryptographic Module contains the following FIPS Approved Algorithms listed in Table 2:

Approved or Allowed Security Functions		Certificate
Symmetric Algorithms		
AES	**(aesasm):** **CBC, ECB** (e/d; 128, 192, 256); **CTR** (ext. only; 128, 192, 256) **CCM** (KS: 128, 192, 256) (Assoc. Data Len Range: 0 - 0, 2^16) (Payload Length Range: 0 - 32 (IV Length(s): 7 8 9 10 11 12 13 (Tag Length(s): 4 6 8 10 12 14 16)	5865 5872

Approved or Allowed Security Functions	Certificate
GCM (KS: AES_128, AES_192, AES_256) (d) Tag Length(s): 128 120 112 104 96 64 32) PT Lengths Tested: (0, 120, 128, 248, 256) ; AAD Lengths tested: (0, 128, 256, 120, 248) ; 96BitIV_Supported **XTS** ((KS: XTS_128, XTS_256) ((e/d) (f))	
(aesgen): **CBC, ECB** (e/d; 128, 192, 256); **CTR** (ext. only; 128, 192, 256) **CCM** (KS: 128, 192, 256) (Assoc. Data Len Range: 0 - 0, 2^16) (Payload Length Range: 0 - 32 (IV Length(s): 7 8 9 10 11 12 13 (Tag Length(s): 4 6 8 10 12 14 16) **GCM** (KS: AES_128, AES_192, AES_256) (d) Tag Length(s): 128 120 112 104 96 64 32) PT Lengths Tested: (0, 128, 256, 120, 248); AAD Lengths tested: (0, 128, 256, 120, 248); 96BitIV_Supported **XTS** ((KS: XTS_128, XTS_256) ((e/d) (f))	5867 5874
aesasm_iiv: **CBC, ECB** (e/d; 128, 192, 256); **CTR** (ext. only; 128, 192, 256) **GCM** (KS: AES_128, AES_192, AES_256) (e)Tag Length(s): 128 96 64) IV Generated: (Internally (using Section 8.2.1)); PT Lengths Tested: (128, 256, 120, 248); AAD Lengths tested: (64, 96); 96BitIV_Supported	5876 5878
aesgen_iiv: **CBC, ECB** (e/d; 128, 192, 256); **CTR** (ext. only; 128, 192, 256) **GCM** (KS: AES_128, AES_192, AES_256)(e) Tag Length(s): 128 96 64) IV Generated: (Internally (using Section 8.2.1)); PT Lengths Tested: (128, 256, 120, 248); AAD Lengths tested: (64, 96); 96BitIV_Supported	5866 5871
aesni: **CBC, ECB** (e/d; 128, 192, 256); **CTR** (ext. only; 128, 192, 256) **CCM** (KS: 128, 192, 256) (Assoc. Data Len Range: 0 - 0, 2^16) (Payload Length Range: 0 - 32 (IV Length(s): 7 8 9 10 11 12 13 (Tag Length(s): 4 6 8 10 12 14 16) **GCM** (KS: AES_128, AES_192, AES_256) (d) Tag Length(s): 128 120 112 104 96 64 32) PT Lengths Tested: (0, 128, 256, 120, 248); AAD Lengths tested: (0, 128, 256, 120, 248); 96BitIV_Supported **XTS** ((KS: XTS_128, XTS_256) ((e/d) (f))	5875 C17
aesni_iiv: **CBC, ECB** (e/d; 128, 192, 256); **CTR** (ext. only; 128, 192, 256)	5870 5877

Approved or Allowed Security Functions		Certificate
	aesni_blkasm: **CBC, ECB** (e/d; 128, 192, 256); **CTR** (ext. only; 128, 192, 256) **GCM** (KS: AES_128, AES_192, AES_256) (d) Tag Length(s): 128 96 64) PT Lengths Tested: (128, 256, 120, 248); AAD Lengths tested: (64, 96); 96BitIV_Supported **XTS** ((KS: XTS_128, XTS_256); ((e/d) (f))	5869 C18
	aesni_blkasm_iiv: **CBC, ECB** (e/d; 128, 192, 256); **CTR** (ext. only; 128, 192, 256) **GCM** (KS: AES_128, AES_192, AES_256) (e) Tag Length(s): 128 96 64) IV Generated: (Internally (using Section 8.2.1)); PT Lengths Tested: (128, 256, 120, 248); AAD Lengths tested: (64, 96); 96BitIV_Supported	5868 5873
Triple DES	**TCBC, TECB** (KO 1 e/d)	2864 2865
Secure Hash Standard (SHS)		
SHS	**Generic C Implementation:** **SHA-1** (BYTE-only) **SHA-224** (BYTE-only) **SHA-256** (BYTE-only) **SHA-384** (BYTE-only) **SHA-512** (BYTE-only)	4652 4653
	shaavx: **SHA-256** (BYTE-only)	4650 4651
	Shaavx2: **SHA-256** (BYTE-only)	4647 4649
	shassse3: **SHA-256** (BYTE-only)	4654 4655
Data Authentication Code		
HMAC	**Generic C Implementation:** **HMAC-SHA1** (Key Size Ranges Tested: KS<BS KS=BS KS>BS) **HMAC-SHA224** (Key Size Ranges Tested: KS<BS KS=BS KS>BS) **HMAC-SHA256** (Key Size Ranges Tested: KS<BS KS=BS KS>BS) **HMAC-SHA384** (Key Size Ranges Tested: KS<BS KS=BS KS>BS) **HMAC-SHA512** (Key Size Ranges Tested: KS<BS KS=BS KS>BS)	3876 3877
	shaavx: **HMAC-SHA256** (Key Size Ranges Tested: KS<BS KS=BS KS>BS)	3874 3875
	Shaavx2: **HMAC-SHA256** (Key Size Ranges Tested: KS<BS KS=BS KS>BS)	3871 3873
	shassse3: **HMAC-SHA256** (Key Size Ranges Tested: KS<BS KS=BS KS>BS)	3878 3879
Asymmetric Algorithms		

Approved or Allowed Security Functions		Certificate
DSA	**shagen:** **FIPS186-4:** SigVer: L = 2048, N = 256 SHA: SHA-256	1491 1492
	shaavx: **FIPS186-4:** SigVer: L = 2048, N = 256 SHA: SHA-256	1489 1490
	shaavx2: **FIPS186-4:** SigVer: L = 2048, N = 256 SHA: SHA-256	1487 1488
	shassse3: **FIPS186-4:** SigVer: L = 2048, N = 256 SHA: SHA-256	1493 1494
Random Number Generation		
DRBG	**CTR DRBG:** **aesasm:** **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128, AES-192, AES-256)	2438 2440
	aesni: **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128, AES-192, AES-256)	2442 C17
	aesgen: **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256)	2439 2441
	Hash DRBG: **shagen:** **Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1, SHA-256, SHA-384, SHA-512)	2458 2459
	shaavx: **Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-256)	2456 2457
	Shaavx2: **Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-256)	2453 2455
	shassse3: **Hash_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-256)	2460 2461
	HMAC DRBG: **shagen:** **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1, SHA-256, SHA-384, SHA-512)	2458 2459

Approved or Allowed Security Functions		Certificate
	shaavx: **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-256)	2456 2457
	Shaavx2: **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-256)	2453 2455
	shassse3: **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-256)	2460 2461
Algorithm used from the Bound NSS module		
HMAC	**HMAC-SHA512** (Key Size Ranges Tested: KS<BS KS=BS KS>BS)	3184 3628

Table 2: FIPS Approved or Allowed Security Functions[1]

3.5 Non-Approved but Allowed Security Functions

The following algorithm is considered non-Approved but allowed to be used in a FIPS-approved mode:

Algorithm	Usage
NDRNG from Linux RNG	Used for seeding NIST SP 800-90A DRBG

Table 3: Non-Approved but Allowed Functions

3.6 Non-Approved Security Functions

The following algorithms are non-Approved and may not be used in a FIPS-approved mode of operation:

Algorithm	Usage
AES-XTS (192 bit)	Encrypt/Decrypt
AES GCM	Encryption with External IV (not meeting IG A.5) or with aesni implementation (KAT not performed) (CAVS tested Certs # 5865, 5872, 5867, 5874, 5875, C17, 5870, 5877, 5869, C18)
DES	Encrypt/Decrypt
SHA-512 (SSSE3, AVX, AVX2 implementation)	Any use of message digest using SHA-512. (CAVS tested Certs # 4650, 4651, 4647, 4649, 4654, 4655, KAT not performed)
ANSI X9.31 RNG	Random number Generation

Table 4: Non-Approved Disallowed Functions

[1] There are some algorithm implementations/modes that were CAVS tested but are not listed in the Table 2 instead are listed in Table 4 as non-approved algorithms as they are not compliant with the FIPS 140-2 requirement."

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

The module can be accessed by utilizing the API it exposes. Table 4 below, shows the mapping of ports and interfaces as per FIPS 140-2 Standard.

FIPS 140-2 Interface	Module Interfaces
Data Input	API input parameters
Data Output	API output parameters
Control Input	API function calls, kernel command line
Status Output	API return codes, kernel logs

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.

ORACLE

6. Operational Environment

6.1 Tested Environments

The module operates in a modifiable operational environment per FIPS 140-2 level 1 specifications. 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	Intel® Xeon ® E5-2699 v4	Oracle Server X6-2
Oracle Linux 6.9 64 bit	Intel® Xeon ® Silver 4114	Oracle Server X7-2

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® Scalable Processors	Cisco UCS B200 M5
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® Scalable Processors	Cisco UCS B480 M5
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® Scalable Processors	Cisco UCS B480 M5
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® Scalable Processors	Cisco UCS C240 M5
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® Scalable Processors	Cisco UCS C480 M5
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

Operating Environment	Processor	Hardware
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
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® Scalable Processors	Fujitsu PRIMERGY CX2560 M4
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® Scalable Processors	Fujitsu PRIMERGY RX2530 M4
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® Scalable Processors	Fujitsu PRIMERGY RX2540 M4
Oracle Linux 6.9 64-bit	Intel® Xeon®E7-4800 v2/E7-8800 v2	Fujitsu PRIMERGY RX4770 M1
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® Scalable Processors	Fujitsu PRIMERGY RX4770 M4
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

Operating Environment	Processor	Hardware
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
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® Scalable 8100/6100/5100/4100/3100 Processors	HPE ProLiant DL360 Gen10
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® Scalable 8100/6100/5100/4100/3100 Processors	HPE ProLiant DL380 Gen10
Oracle Linux 6.9 64-bit	Intel® Xeon®E5-4600 v3 & v4	HPE ProLiant DL560 Gen9
Oracle Linux 6.9 64-bit	Intel® Xeon® Scalable 8170 Processors	HPE ProLiant DL560 Gen10
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

Operating Environment	Processor	Hardware
Oracle Linux 6.9 64-bit	Intel® Xeon® Scalable 8100/6100/5100/4100/3100 Processors	HPE Synergy 480 Gen10 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® Scalable 8100/6100/5100 Processors	HPE Synergy 660 Gen10 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® Scalable Processors	Huawei FusionServer 1288H V5
Oracle Linux 6.9 64-bit	Intel® Xeon® Scalable Processors	Huawei FusionServer 2288H V5
Oracle Linux 6.9 64-bit	Intel® Xeon® Scalable Processors	Huawei FusionServer CH121 V5
Oracle Linux 6.9 64-bit	Intel® Xeon® Scalable Processors	Huawei FusionServer CH121L V5
Oracle Linux 6.9 64-bit	Intel® Xeon® Scalable Processors	Huawei FusionServer CH242 V5
Oracle Linux 6.9 64-bit	Intel® Xeon® E5-2600 v3 & v4	Huawei FusionServer RH2288H V3
Oracle Linux 6.9 64-bit	Intel® Xeon® Scalable Processors	Huawei FusionServer XH321 V5
Oracle Linux 6.9 64-bit	Intel® Xeon® E5-2600 v3	Inspur Yingxin NF5180M4
Oracle Linux 6.9 64-bit	Intel® Xeon® Scalable Processors	Inspur Yingxin NF5180M5
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® Scalable Processors	Inspur Yingxin NF5180M5
Oracle Linux 6.9 64-bit	Intel® Xeon® E5-2600 v3 & v4	Inspur Yingxin NF5280M4
Oracle Linux 6.9 64-bit	Intel® Xeon® Scalable Processors	Inspur Yingxin NF5280M5
Oracle Linux 6.9 64-bit	Intel® Xeon® E5-2600 v3 & v4	Inspur Yingxin NF5460M4
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
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 v3	Oracle Server X5-2L
Oracle Linux 6.9 64-bit	Intel® Xeon® E7-8800 v3	Oracle Server X5-4
Oracle Linux 6.9 64-bit	Intel® Xeon® E7-8800 v3	Oracle ServerX5-8
Oracle Linux 6.9 64-bit	Intel® Xeon® E5-2600 v4	Oracle Server X6-2
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® Scalable 8100/6100/4100 Processors	Oracle Server X7-2
Oracle Linux 6.9 64-bit	Intel® Xeon® Scalable 8100/6100/4100 Processors	Oracle Server X7-2L
Oracle Linux 6.9 64-bit	Intel® Xeon® Scalable 8100/6100 Processors	Oracle Server X7-8
Oracle Linux 6.9 64-bit	Intel® Xeon® x7500-series	Oracle Sun Fire X4470
Oracle Linux 6.9 64-bit	Intel® Xeon® x7500-series	Oracle Sun Fire X4800

Operating Environment	Processor	Hardware
Oracle Linux 6.9 64-bit	Intel® Xeon® E7-8800	Oracle Sun Server X2-8
Oracle Linux 6.9 64-bit	Intel® Xeon® E7-4800	Oracle Sun Server X2-4
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
Oracle Linux 6.9 64-bit	Intel® Xeon® E7-8800 v2	Oracle Sun Server X4-4
Oracle Linux 6.9 64-bit	Intel® Xeon® E7-8800 v2	Oracle Sun Server X4-8

Table 7: Vendor Affirmed Operational Environments

Note: CMVP makes no statement as to the correct operation of the module 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 that request cryptographic services is the single user of the module.

In operational 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 symmetric encryption/decryption, keyed hash, message digest, random number generation, show status, zeroization.
- **Crypto Officer Role**: performs the module installation and configuration, module's initialization, self-tests.

7.2 FIPS Approved Operator Services and Descriptions

The below table provides a full description of FIPS Approved services provided by the module and lists the roles allowed to invoke each service.

U	CO	Service Name	Service Description	Keys and CSP(s)	Access Type(s)
X		Symmetric Encryption/Decryption	Encrypts or decrypts a block of data using 3-Key Triple-DES or AES in FIPS mode	AES or 3-Key Triple-DES Key	R, W, X
X		Keyed Hash (HMAC)	Sign and or authenticate data using HMAC-SHA	HMAC Key	R, W, X
X		Message Digest	Hash a block of data.	None	N/A
X		Random Number Generation	Generate random numbers based on the NIST SP 800-90A Standard	Entropy input string and seed	R, W, X
X		Authenticated Encryption	Encrypt-then-MAC cipher (authenc) used for IPsec	AES key, HMAC key	R, W, X
X		Show Status	Show status of the module state via verbose mode, exit codes and kernel logs (dmesg)	None	N/A
	X	Self-Test	Initiate power-on self-tests	None	N/A
X		Zeroize	Zeroize all critical security parameters	All keys and CSP's	Z
	X	Module Initialization	Initialize the module into the FIPS Approved Mode	None	N/A
	X	Installation and Configuration	Install and configure the module.	None	N/A
X		Error detection code[2]	Error detection code using crc32c, crct10dif	None	N/A

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

Table 8: FIPS Approved Operator Services and Descriptions

[2] The algorithms used in this service do not provide cryptographic attribute.

7.3 Non-FIPS Approved Services and Descriptions

The following table lists the non-Approved services available in non-FIPS mode.

U	CO	Service Name	Service Description	Keys and CSP(s)	Access Type(s)
X		Symmetric Encryption/Decryption	Encrypts or decrypts using non-Approved algorithms listed in Table 4	AES, DES key	R, W, X
X		Random Number Generation	Generation of random numbers using the ANSI X9.31 PRNG	None	N/A
X		Message Digest	Hashing using non-validated hash functions listed in Table 4	None	N/A
X		Keyed Hash	HMAC Keys < 112 bits.	HMAC keys < 112 bits.	R, W, X

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

Table 9: Non-FIPS Approved Operator Services and Descriptions

7.4 Operator Authentication

The module is a Level 1 software-only cryptographic module and does not implement authentication. The role is implicitly assumed based on the service requested.

8. Key and CSP Management

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

CSP Name	Generation	Entry/Output	Storage	Zeroization
AES Keys (128, 192, 256 bits)	N/A	Key is passed into the module via API input parameter	kernel memory	Memory is automatically overwritten by zeroes when freeing the cipher handler
Triple-DES Keys (192 bits)	N/A	Key is passed into the module via API input parameter	kernel memory	Memory is automatically overwritten by zeroes when freeing the cipher handler
DRBG Entropy Input String	Obtained from NDRNG	N/A	kernel memory	Memory is automatically overwritten by zeroes when freeing the cipher handler
DRBG internal state (V, key and C values	Derived from Entropy input as defined in NIST SP 800-90A	N/A	kernel memory	Memory is automatically overwritten by zeroes when freeing the cipher handler
HMAC Key (≥ 112 bits)	N/A	Key is passed into the module via API input parameter	kernel memory	Memory is automatically overwritten by zeroes when freeing the cipher handler

Table 10: CSP Table

8.1 Random Number Generation

The module employs the Deterministic Random Bit Generator (DRBG) based on [SP800-90A] for the creation of random numbers. The DRBG supports the Hash_DRBG, HMAC_DRBG and CTR_DRBG mechanisms. The DRBG is initialized during module initialization. The module loads by default the DRBG using HMAC DRBG with SHA-512, without prediction resistance. To seed the DRBG, the module uses a Non-Deterministic Random Number Generator (NDRNG) as the entropy source. The NDRNG provides at least 130 bits of entropy to the DRBG during initialization (seed) and reseeding (reseed). The module performs continuous random number generator test on the output of NDRNG to ensure that consecutive random numbers do not repeat, and performs DRBG health tests as defined in section 11.3 of [SP800-90A]. CAVEAT: The module generates random strings whose strengths are modified by available entropy.

The module does not provide any key generation service or perform key generation for any of its Approved algorithms. Keys are passed in from calling application via API parameters.

8.2 Key Entry/Output

The keys are provided to the module via API input parameters in plaintext form. The keys are not transmitted beyond the physical boundary. The module does not support manual key entry.

8.3 Key/CSP Storage

Symmetric keys are provided to the module by the calling process, and are destroyed when released by the appropriate API function calls. The module does not perform persistent storage of keys. The DSA public key used for signature verification is stored as part of the module and relies on the operating system for its protection.

8.4 Key/CSP Zeroization

The application that uses the module is responsible for appropriate destruction and zeroization of the key material. The library provides functions for key allocation and destruction. When a calling kernel components calls the appropriate API function that operation overwrites memory with 0's and then frees that memory.

ORACLE

9. 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, the module performs conditional test for NDRNG. On successful completion of the power-up tests, the module is operational and the crypto services are available. A failure of any of the self-tests panics the kernel and no crypto operations are possible. The only recovery is to reboot the module. See section 10.3 for details.

9.1 Power-Up Self-Tests

The module performs power-up self-tests at module initialization without operator intervention. While the module is performing the power-up tests, services are not available and input or output is not possible. The on-demand power up self-tests can be performed by power cycling the Module or by rebooting the operating system. The table below summarizes the power-on self-tests performed by the module. If the known answer does not match the test fails. The different implementations of the same algorithms listed in Table 2 are tested separately by performing the known-answer tests using the same test vectors.

Algorithm	Test
AES	KAT, encryption and decryption are tested separately.
Triple-DES	KAT, encryption and decryption are tested separately.
DSA Signature Verification[3]	Part of the integrity test (considered as a KAT)
SP 800-90A CTR_DRBG	KAT
SP 800-90A Hash_DRBG	KAT
SP 800-90A HMAC_DRBG	KAT
SHA	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 KAT
HMAC	HMAC-SHA-1, HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512 KAT
Module Integrity	Performed by sha512hmac application with HMAC-SHA-512 provided by NSS

Table 11: Power-On Self-Tests

9.1.1 Integrity Tests

The integrity of the static kernel binary is performed by sha512hmac application using HMAC-SHA-512. At run time, the module invokes the sha512hmac utility to calculate the HMAC value of the static kernel binary file and then compares it with the pre-stored HMAC file in /boot/.vmlinuz-$(uname -r).hmac.

The sha512hmac application performs its own integrity check by calculating the HMAC value of its binary and comparing it to the HMAC value stored in sha512hmac.hmac. The HMAC-SHA-512 algorithm is provided by the bound NSS module and is KAT tested before the NSS module makes itself available to the sha512hmac application.

The Oracle Linux UEK object files (*. ko referenced in section 3.1) loaded into the Linux kernel during boot time are checked with the DSA signature verification implementation of the Linux kernel to confirm their integrity. If the HMAC values do not match or the DSA signature verification fails the kernel panics indicating error state. When the self-test of these object files passes, it implies that the integrity check passed as well.

[3] The DSA signature verification is only used as part of integrity test and is not available as a service from the module.

9.2 Conditional Self-Tests

The module performs conditional tests on the cryptographic algorithms shown in the following table:

Algorithm	Test
NDRNG	The module performs conditional self-tests on the output of NDRNG.

Table 12: Conditional Self-Tests

10. Crypto-Officer and User Guidance

This section provides guidance for the Cryptographic Officer and the User to maintain proper use of the module per FIPS 140-2 requirements.

10.1 Crypto-Officer Guidance

To operate the Kernel Crypto API module, the operating system must be restricted to a single operator mode of operation. (This should not be confused with single user mode which is runlevel 1 on Oracle Linux. This refers to processes having access to the same cryptographic instance which Oracle Linux ensures cannot happen by the memory management hardware.)

10.1.1 Secure Installation and Startup

Crypto Officers use the Installation instructions to install the Module in their environment. The version of the RPM containing the FIPS validated module is stated in section 3.1 above.

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.

To configure the operating environment to support FIPS perform the following steps:

1. Install the dracut-fips package:
   # yum install dracut-fips
2. Recreate the INITRAMFS image:
   # dracut -f

After regenerating the initramfs, the Crypto Officer has to append the following string to the kernel command line by changing the setting in the boot loader:

fips=1

If /boot or /boot/efi resides on a separate partition, the kernel parameter boot=<partition of /boot or /boot/efi> must be supplied. The partition can be identified with the command "df /boot" or "df /boot/efi" respectively. For example:

$ df /boot

Filesystem	1K-blocks	Used	Available	Use	Mounted on
/dev/sda1	233191	30454	190296	14%	/boot

The partition of /boot is located on /dev/sda1 in this example. Therefore, the following string needs to be appended to the kernel command line:

boot=/dev/sda1

10.1.2 FIPS 140-2 and AES NI Support

According to the Kernel Crypto API FIPS 140-2 Security Policy, the Kernel Crypto API module supports the AES-NI Intel processor instruction set as an approved cipher. The AES-NI instruction set is used by the Module.

In case you configured a full disk encryption using AES, you *may* use the AES-NI support for a higher performance compared to the software-only implementation.
To utilize the AES-NI support, the mentioned Module must be loaded during boot time by installing a plugin.

Before you install the plugin, you MUST verify that your processor offers the AES-NI instruction set by calling the following command:

```
cat /proc/cpuinfo | grep aes
```

If the command returns a list of properties, including the “aes” string, your CPU provides the AES-NI instruction set. If the command returns nothing, AES-NI is not supported.

You MUST NOT install the following plugin if your CPU does not support AES-NI because the kernel will panic during boot.

The support for the AES-NI instruction set during boot time is enabled by installing the following plugin (make sure that the version of the plugin RPM matches the version of the installed RPMs!):

```
# install the dracut-fips-aesni package
yum install dracut-fips-aesni-*.noarch.rpm
# recreate the initramfs image
dracut –f
```

The changes come into effect during the next reboot.

10.2 User Guidance

CTR and RFC3686 mode must only be used for IPsec. It must not be used otherwise.

There are three implementations of AES: aes-generic, aesni-intel, and aes-x86_64 on x86_64 machines. The additional specific implementations of AES for the x86 architecture are disallowed and not available on the test platforms.

When using the Module, the user shall utilize the Linux Kernel Crypto API provided memory allocation mechanisms. In addition, the user shall not use the function copy_to_user() on any portion of the data structures used to communicate with the Linux Kernel Crypto API.

Only the cryptographic mechanisms provided with the Linux Kernel Crypto API are considered for use. The NSS bound module, although used, is only considered to support the integrity verification and is not intended for general-purpose use with respect to this Module.

10.2.1 AES-XTS Usage

The XTS mode must only be used for the disk encryption functionality offered by dm-crypt.

10.2.2 AES-GCM Usage

The GCM with internal IV generation in FIPS mode is in compliance with RFC4106 and shall only be used in conjunction with the IPsec stack of the kernel to be compliant with IG A.5. Any other usage of GCM will be considered non-Approved. In case the module's power is lost and then restored, the key used for the AES GCM shall be redistributed.

10.2.3 Triple-DES Usage

According to IG A.13, the same Triple-DES key shall not be used to encrypt more than 2^16 64-bit blocks of data.

10.3 Handling Self-Test Errors

The Module transition to error state when any of self-test or conditional test fails. In error state, the kernel is in a panicked state and the operating system will not load. As such, the output is inhibited and no crypto operations are available in the error state. In order to recover from the error, the module needs to rebooted. If the failure continues, the module needs to be reinstalled.

The kernel dumps self-test success and failure messages into the kernel message ring buffer. Post boot, the messages are moved to /var/log/messages.

Use **dmesg** to read the contents of the kernel ring buffer. The format of the ring buffer (**dmesg**) output is:

alg: self-tests for %s (%s) passed

Typical messages are similar to "alg: self-tests for xts(aes) (xts(aes-x86_64)) passed" for each algorithm/sub-algorithm type.

11. Mitigation of Other Attacks

The module does not claim to mitigate against any attacks.

Acronyms, Terms and Abbreviations

Term	Definition
AES	Advanced Encryption Standard
CAVP	Cryptographic Algorithm Validation Program
CMVP	Cryptographic Module Validation Program
CSE	Communications Security Establishment
CSP	Critical Security Parameter
DH	Diffie-Hellman
DHE	Diffie-Hellman Ephemeral
DRBG	Deterministic Random Bit Generator
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EDC	Error Detection Code
HMAC	(Keyed) Hash Message Authentication Code
IKE	Internet Key Exchange
KAT	Known Answer Test
KDF	Key Derivation Function
NIST	National Institute of Standards and Technology
PAA	Processor Algorithm Acceleration
PBKDF	Password Based Key Derivation Function
POST	Power On Self Test
PR	Prediction Resistance
PSS	Probabilistic Signature Scheme
PUB	Publication
SHA	Secure Hash Algorithm
TLS	Transport Layer Security

Table 13: 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 https://www.oracle.com/linux/ .

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
FIPS PUB 140-2 Annex A	NIST	FIPS 140-2 Annex A: Approved Security Functions
FIPS PUB 140-2 Annex B	NIST	FIPS 140-2 Annex B: Approved Protection Profiles
FIPS PUB 140-2 Annex C	NIST	FIPS 140-2 Annex C: Approved Random Number Generators
FIPS PUB 140-2 Annex D	NIST	FIPS 140-2 Annex D: Approved Key Establishment Techniques
DTR for FIPS PUB 140-2	NIST	Derived Test Requirements (DTR) for FIPS PUB 140-2, Security Requirements for Cryptographic Modules
NIST SP 800-67	NIST	Recommendation for the Triple Data Encryption Algorithm TDEA Block Cypher
FIPS PUB 197	NIST	Advanced Encryption Standard
FIPS PUB 198-1	NIST	The Keyed Hash Message Authentication Code (HMAC)
FIPS PUB 186-4	NIST	Digital Signature Standard (DSS)
FIPS PUB 180-4	NIST	Secure Hash Standard (SHS)
NIST SP 800-131A	NIST	Recommendation for the Transitioning of Cryptographic Algorithms and Key Sizes

Table 14: References