

**ORACLE®**

Linux

## FIPS 140-2 Non-Proprietary Security Policy

---

### Oracle Linux Unbreakable Enterprise Kernel (UEK 5) Cryptographic Module

FIPS 140-2 Level 1 Validation

Software Version: R7-5.0.0

Date: September 22, 2023



**Title:** Oracle Linux Unbreakable Enterprise Kernel Cryptographic Module Security Policy

**Date:** September 22, 2023

**Author:** Oracle Security Evaluations – Global Product Security

**Contributing Authors:**

Oracle Linux Engineering

Acumen Security

Oracle Corporation  
World Headquarters  
2300 Oracle Way  
Austin, TX 78741  
U.S.A.

Worldwide Inquiries:

Phone: +1.650.506.7000

Sales: 1-800-672-2531

[www.oracle.com](http://www.oracle.com)

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

Copyright © 2023, 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**



## TABLE OF CONTENTS

Section	Title	Page
<b>1.</b>	<b>Introduction .....</b>	<b>1</b>
1.1	Overview.....	1
1.2	Document Organization .....	1
<b>2.</b>	<b>Oracle Linux Unbreakable Enterprise Kernel Cryptographic Module .....</b>	<b>2</b>
2.1	Functional Overview.....	2
2.2	FIPS 140-2 Validation Scope .....	2
<b>3.</b>	<b>Cryptographic Module Specification .....</b>	<b>3</b>
3.1	Definition of the Cryptographic Module .....	3
3.2	Definition of the Physical Cryptographic Boundary .....	4
3.3	Modes of Operation .....	4
3.4	Approved or Allowed Security Functions .....	5
3.5	Non-Approved but Allowed Security Functions .....	9
3.6	Non-Approved Security Functions.....	9
<b>4.</b>	<b>Module Ports and Interfaces .....</b>	<b>10</b>
<b>5.</b>	<b>Physical Security .....</b>	<b>11</b>
<b>6.</b>	<b>Operational Environment.....</b>	<b>12</b>
6.1	Tested Environments.....	12
6.2	Vendor Affirmed Environments.....	12
6.3	Vendor Affirmed Environments.....	16
<b>7.</b>	<b>Roles, Services and Authentication.....</b>	<b>17</b>
7.1	Roles .....	17
7.2	FIPS Approved Operator Services and Descriptions.....	17
7.3	Non-FIPS Approved Services and Descriptions.....	18
7.4	Operator Authentication .....	18
<b>8.</b>	<b>Key and CSP Management .....</b>	<b>19</b>
8.1	Random Number Generation .....	19
8.2	Key Entry/Output.....	20
8.3	Key/CSP Storage .....	20
8.4	Key/CSP Zeroization.....	20
<b>9.</b>	<b>Self-Tests.....</b>	<b>21</b>
9.1	Power-Up Self-Tests .....	21
9.1.1	Integrity Tests .....	21
9.2	Conditional Self-Tests .....	22
<b>10.</b>	<b>Crypto-Officer and User Guidance .....</b>	<b>23</b>
10.1	Crypto-Officer Guidance.....	23
10.1.1	Secure Installation and Startup .....	23
10.1.2	FIPS 140-2 and AES NI Support.....	25
10.2	User Guidance .....	26
10.2.1	AES-XTS Usage .....	26
10.2.2	AES-GCM Usage .....	26
10.2.3	Triple-DES Usage.....	26
10.3	Handling Self-Test Errors .....	27

11. Mitigation of Other Attacks.....	28
Acronyms, Terms and Abbreviations .....	29
References .....	30

## List of Tables

Table 1: FIPS 140-2 Security Requirements.....	2
Table 2: FIPS Approved or Allowed Security Functions .....	8
Table 3: Non-Approved but Allowed Security Functions .....	9
Table 4: Non-Approved Security Functions .....	9
Table 5: Mapping of FIPS 140 Logical Interfaces to Logical Ports .....	10
Table 6: Tested Operating Environment.....	12
Table 7: Vendor Affirmed Operating Environment .....	16
Table 8: FIPS Approved Operator Services and Descriptions .....	17
Table 9: Non-FIPS Approved Operator Services and Descriptions.....	18
Table 10: CSP Table .....	19
Table 11: Power-On Self-Tests .....	21
Table 12: Conditional Self-Tests.....	22
Table 13: Acronyms.....	29
Table 14: References .....	30

## List of Figures

Figure 1: Oracle Linux UEK Logical Cryptographic Boundary.....	4
Figure 2: Oracle Linux UEK Hardware Block Diagram .....	4



## 1. Introduction

### 1.1 Overview

The Unbreakable Enterprise Kernel (UEK 5), included as part of Oracle Linux, provides the latest open source innovations, key optimizations and security for enterprise cloud workloads. This Linux kernel powers Oracle Cloud and Oracle Engineered Systems such as Oracle Exadata Database Machine. Oracle tests UEK intensively with demanding Oracle workloads, and recommends UEK for Oracle deployments and all other enterprise deployments.

Oracle contributes to upstream Linux kernel development with enhancements that benefit Oracle Database, middleware, applications and hardware, as well as our broad partner ecosystem. These enhancements are distributed to customers through UEK for Oracle Linux.

By selectively integrating the latest open source Linux capabilities into UEK while still providing application binary compatibility with the Red Hat Compatible Kernel, Oracle makes it easy to run the most demanding cloud and enterprise workloads without compromising stability and security. We test all our on-premises software, and run Oracle Cloud on UEK, ensuring you can achieve the highest scalability and performance with your current workloads and those of the future.

This document is the Security Policy for the Oracle Linux Unbreakable Enterprise Kernel (UEK 5) Cryptographic Module by Oracle Corporation. Oracle Linux UEK 5 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 UEK 5 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 UEK 5 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/CCCS 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 Security Policy document is one document in a FIPS 140-2 Submission Package. In addition to this document, the Submission Package contains:

- Oracle Linux Unbreakable Enterprise Kernel (UEK 5) 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 Unbreakable Enterprise Kernel Cryptographic Module

### 2.1 Functional Overview

The Oracle Linux Unbreakable Enterprise Kernel Cryptographic Module is a software only cryptographic module that provides general-purpose cryptographic services to the remainder of the Linux kernel. The Oracle Linux UEK 5 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 UEK 5 Cryptographic Module is a 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 binary 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 version R7-5.0.0 running on Oracle Linux 7.6 to operate are defined below:

- Oracle Linux Unbreakable Enterprise Kernel Cryptographic Module with the version of the RPM file [kernel-uek-4.14.35-1902.300.11.el7uek.x86\\_64.rpm](#).
- The configuration of the FIPS mode is provided by the dracut-fips version [dracut-fips-033-568.0.1.el7.x86\\_64.rpm](#) and dracut-fips-aesni package with the version [dracut-fips-aesni-033-568.0.1.el7.x86\\_64.rpm](#).

The following component acts as bound modules need to be installed for the Oracle Linux 7 UEK 5 Cryptographic Module to operate:

- The bound module Oracle Linux 7 NSS Cryptographic Library with FIPS 140-2 Certificate #[4586](#) (hereafter referred to as the “NSS module”) provides 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) file.

The Oracle Linux UEK 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 loadable components `/lib/modules/$(uname -r)/kernel/crypto/*.ko`
- kernel loadable components `/lib/modules/$(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`

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

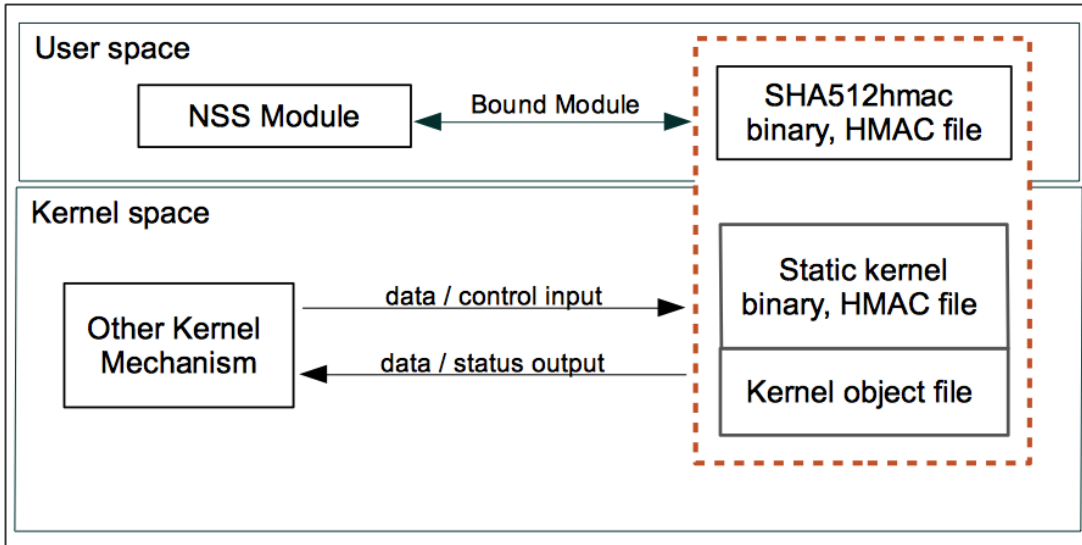


Figure 1: Oracle Linux UEK Logical Cryptographic Boundary

### 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.

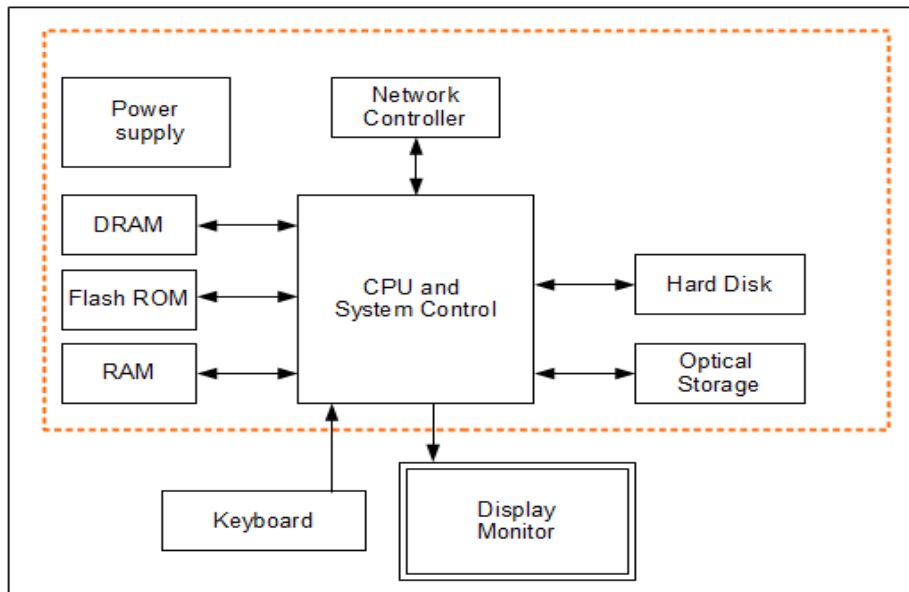


Figure 2: Oracle Linux UEK Hardware Block Diagram

### 3.3 Modes of Operation

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

Section 10 describes the Crypto Officer and User Guidance to correctly install, configure, and use the module in the FIPS Approved mode of operation. The module turns to FIPS Approved mode after correct initialization and 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. The critical security parameters (CSPs) used or stored in approved mode are not used in non-approved mode and vice versa. Once the module is operational, the mode of operation is implicitly assumed depending on the security function invoked and the security strength of the cryptographic keys.

The Approved services available in FIPS mode can be found in section 7.2, Table 8. The non-approved services not available in FIPS mode can be found in section 7.3, Table 9.

### 3.4 Approved or Allowed Security Functions<sup>1</sup>

The Oracle Linux UEK Cryptographic Module contains the following FIPS Approved Algorithms:

Approved or Allowed Security Functions		Certificate
<i>Symmetric Algorithms</i>		
AES	<p><b>(aesasm):</b>  <b>CBC, ECB</b> (e/d; 128, 192, 256);  <b>CTR</b> (ext. only; 128, 192, 256)  <b>CCM</b> (KS: 128, 192, 256)            Assoc. Data Len Range: 0 - 0, 2<sup>16</sup>            Payload Length Range: 0 - 32            IV Length(s): 56, 64, 72, 80, 88, 96, 104 (bits)            (Tag Length(s): 32, 48, 64, 80, 96, 112, 128 (bits)  <b>XTS</b> ((KS: XTS_128, XTS_256) ((e/d) (f))</p>	<a href="#">C 1733</a>
	<p><b>aesni:</b>  <b>CBC, ECB</b> (e/d; 128, 192, 256);  <b>CTR</b> (ext. only; 128, 192, 256)  <b>CCM</b> (KS: AES_128, AES_192, AES_256) (d)            Tag Length(s): 32, 48, 64, 80, 96, 112, 128)            IV Length (56, 64, 72, 80, 88, 96, 104)            PT Lengths Tested: (0-32);            AAD Lengths tested: (0-65536);  <b>GCM</b> (KS: AES_128, AES_192, AES_256) (e/d)            Tag Length(s): 32, 64, 96, 104, 112, 120, 128)            PT Lengths Tested: (0, 120, 128, 248, 25);            AAD Lengths tested: (0, 120, 128, 248, 256);            96 Bit IV_Supported  <b>GMAC</b> (KS: AES_128, AES_192, AES_256) (e/d)            Tag Length(s): 64, 96, 128)            AAD Lengths tested: (0, 64, 96);            96 Bit IV            IV Generation: External  <b>XTS</b> ( (KS: XTS_128, XTS_256); ( (e/d) (f) )</p>	<a href="#">C 1735</a>
	<p><b>aesni_blkasm:</b>  <b>CBC, ECB</b> (e/d; 128, 192, 256);</p>	<a href="#">C 1736</a>

<sup>1</sup> There are algorithms, modes, and keys that have been CAVs tested but not used by the module. Only the algorithms, modes/methods, and key lengths/curves/moduli shown in this table are used by the module

Approved or Allowed Security Functions		Certificate
	<p><b>CTR</b> (ext. only; 128, 192, 256)  <b>GCM</b> (KS: AES_128, AES_192, AES_256) (e/d)            Tag Length(s): 64, 96, 128)            PT Lengths Tested: (120, 128, 248, 256);            AAD Lengths tested: (64, 96);            96BitIV_Supported  <b>GMAC</b> (KS: AES_128, AES_192, AES_256) (e/d)            Tag Length(s): 64, 96, 128)            AAD Lengths tested: (0, 64, 96);            96 Bit IV            IV Generation: External  <b>XTS</b> ((KS: XTS_128, XTS_256); ((e/d) (f)))</p>	
	<p><b>aesgen</b>  <b>CBC, ECB</b> (e/d; 128, 192, 256);  <b>CTR</b> (ext. only; 128, 192, 256)  <b>CCM</b> (KS: AES_128, AES_192, AES_256) (e/d)            Tag Length(s): 32, 48, 64, 80, 96, 112, 128)            IV Length (56, 64, 72, 80, 88, 96, 104)            PT Lengths Tested: (0-32);            AAD Lengths tested: (0-65536);  <b>GCM</b> (KS: AES_128, AES_192, AES_256) (e/d)            Tag Length(s): 32, 64, 96, 104, 112, 120, 128)            PT Lengths Tested: (0, 120, 128, 248, 256);            AAD Lengths tested: (0, 120, 128, 248, 256);            96 Bit IV Supported  <b>GMAC</b> (KS: AES_128, AES_192, AES_256) (e/d)            Tag Length(s): 64, 96, 128)            AAD Lengths tested: (0, 64, 96);            96 Bit IV            IV Generation: External  <b>XTS</b> ((KS: XTS_128, XTS_256); ((e/d) (f)))</p>	<a href="#">C 1734</a>
Triple DES	<p><b>C Implementation</b>  <b>TCBC, TECB</b> (KO 1 e/d);  <b>CTR</b> ( ext only )</p>	<a href="#">C 1741</a>
	<p><b>BLK ASM Implementation</b>  <b>TCBC, TECB</b> (KO 1 e/d);  <b>CTR</b> (ext only)</p>	<a href="#">C 1737</a>
<b>Secure Hash Standard (SHS)</b>		
SHS	<p><b>Generic C Implementation:</b>  <b>SHA-1</b> (BYTE-only)  <b>SHA-224</b> (BYTE-only)  <b>SHA-256</b> (BYTE-only)  <b>SHA-384</b> (BYTE-only)  <b>SHA-512</b> (BYTE-only)</p>	<a href="#">C 1739</a>
	<p><b>shaavx:</b>  <b>SHA-1</b> (BYTE-only)  <b>SHA-224</b> (BYTE-only)  <b>SHA-256</b> (BYTE-only)  <b>SHA-384</b> (BYTE-only)</p>	<a href="#">C 1738</a>

Approved or Allowed Security Functions		Certificate
	SHA-512 (BYTE-only)	
	<b>shaavx2:</b> SHA-1 (BYTE-only) SHA-224 (BYTE-only) SHA-256 (BYTE-only) SHA-384 (BYTE-only) SHA-512 (BYTE-only)	<a href="#">C 1744</a>
	<b>shasse3:</b> SHA-1 (BYTE-only) SHA-224 (BYTE-only) SHA-256 (BYTE-only) SHA-384 (BYTE-only) SHA-512 (BYTE-only)	<a href="#">C 1740</a>
<b>Data Authentication Code</b>		
HMAC	<b>Generic C Implementation:</b> 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 )	<a href="#">C 1739</a>
	<b>shaavx:</b> 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 )	<a href="#">C 1738</a>
	<b>shaavx2:</b> 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 )	<a href="#">C 1744</a>
	<b>shasse3:</b> 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 )	<a href="#">C 1740</a>
	<b>Oracle Linux 7 NSS without AES-NI</b> HMAC-SHA512 (Key Size Ranges Tested: KS<BS KS=BS KS>BS ) Used for module integrity test	<a href="#">C 786</a>
<b>Asymmetric Algorithms</b>		
RSA	<b>shagen:</b> <b>FIPS186-4:</b> ALG[RSASSA-PKCS1_V1_5] SIG(Ver) (2048 SHA (1, 224, 256, 384, 512)) (3072 SHA (1, 224, 256, 384, 512))	<a href="#">C 1739</a>

Approved or Allowed Security Functions		Certificate
	<b>shaavx:</b> <b>FIPS186-4:</b> ALG[RSASSA-PKCS1_V1_5] SIG(Ver) (2048 SHA (1, 256, 384, 512)) (3072 SHA (1, 256, 384, 512))	<a href="#">C 1738</a>
	<b>shaavx2:</b> <b>FIPS186-4:</b> ALG[RSASSA-PKCS1_V1_5] SIG(Ver) (2048 SHA (1, 224, 256, 384, 512)) (3072 SHA (1, 224, 256, 384, 512))	<a href="#">C 1744</a>
	<b>shasse3:</b> <b>FIPS186-4:</b> ALG[RSASSA-PKCS1_V1_5] SIG(Ver) (2048 SHA (1, 256, 512 )) (3072 SHA (1, 256 , 512))	<a href="#">C 1740</a>
<b>Random Number Generation</b>		
DRBG	<b>CTR DRBG:</b> <b>aesasm:</b> <b>CTR_DRBG:</b> [ Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: ( AES-128, AES-192, AES-256 )	<a href="#">C 1733</a>
	<b>aesni:</b> <b>CTR_DRBG:</b> [ Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: ( AES-128, AES-192, AES-256)	<a href="#">C 1735</a>
	<b>aesgen:</b> <b>CTR_DRBG:</b> [ Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: ( AES-128 , AES-192 , AES-256 )	<a href="#">C 1734</a>
	<b>Hash DRBG and HMAC DRBG :</b> <b>shagen:</b> <b>Hash_Based DRBG:</b> [ Prediction Resistance Tested: Enabled and Not Enabled ( SHA-1, SHA-256, SHA-384, SHA-512) <b>HMAC_Based DRBG:</b> [ Prediction Resistance Tested: Enabled and Not Enabled (SHA-1, SHA-256, SHA-384, SHA-512)	<a href="#">C 1739</a>
	<b>Shaavx2:</b> <b>Hash_Based DRBG:</b> [ Prediction Resistance Tested: Enabled and Not Enabled (SHA-1, SHA-256, SHA-384, SHA-512) <b>HMAC_Based DRBG:</b> [ Prediction Resistance Tested: Enabled and Not Enabled (SHA-1, SHA-256, SHA-384, SHA-512)	<a href="#">C 1744</a>
	<b>shasse3:</b> <b>Hash_Based DRBG:</b> [ Prediction Resistance Tested: Enabled and Not Enabled (SHA-1, SHA-256, SHA-384, SHA-512) <b>HMAC_Based DRBG:</b> [ Prediction Resistance Tested: Enabled and Not Enabled (SHA-1, SHA-256, SHA-384, SHA-512)	<a href="#">C 1740</a>
	<b>shaavx:</b> <b>Hash_Based DRBG:</b> [ Prediction Resistance Tested: Enabled and Not Enabled (SHA-1, SHA-256, SHA-384, SHA-512) <b>HMAC_Based DRBG:</b> [ Prediction Resistance Tested: Enabled and Not Enabled (SHA-1, SHA-256, SHA-384, SHA-512)	<a href="#">C 1738</a>

**Table 2: FIPS Approved or Allowed Security Functions**



The module also claims SP 800-38F compliant key wrapping with the following modes (using any available implementations specified in Table 2):

- AES-GCM
- AES-CCM
- AES-CBC with HMAC-SHA1, HMAC-SHA-256 or HMAC-SHA-512.

The following caveats apply:

KTS (AES Certs. C 1733, C 1734, C 1735, and C 1736 key establishment methodology provides between 128 and 256 bits of encryption strength)

KTS (AES Certs C 1733, C 1734, C 1735, and C 1736 and HMAC Certs. C 1738, C 1739, C 1740 and C 1744, key establishment methodology provides between 128 and 256 bits of encryption strength)

### 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	Used for seeding NIST SP 800-90A DRBG

**Table 3: Non-Approved but Allowed Security Functions**

### 3.6 Non-Approved Security Functions

The following algorithms are considered non-Approved and may not be used in a FIPS-approved mode of operation. The services associated with these algorithms are specified in section 7.3.

Algorithm	Usage
AES-XTS (192 bit)	Encrypt/Decrypt
DES	Encrypt/Decrypt
ChaCha20	Encryption/Decryption and Random Number Generation
SHA-1 (multiple-buffer)	Per IG G.13 “non-compliant”
Poly 1305	Hashing
HMAC	HMAC Keys less than 112 bits
ANSI X9.31 RNG	Random Number Generation

**Table 4: Non-Approved Security Functions**

## 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 below, shows the mapping of ports and interfaces as per FIPS 140-2 Standard.

FIPS 140 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.

## 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:

Module Version	Operating Environment	Processor	Hardware
R7-5.0.0	Oracle Linux 7.6 64 bit	Intel® Xeon® Silver 4114	Oracle Server X7-2
R7-5.0.0	Oracle Linux 7.6 64 bit	AMD® EPYC® 7551	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 7.6 64-bit	Intel® Xeon® 8167M	Oracle X7-2
Oracle Linux 7.6 64-bit	AMD® EPYC® 7742	Oracle X7-2
Oracle Linux 7.6 64-bit	Intel® Xeon® E5-2600/E5-2600 v2	Cisco UCS B200 M3
Oracle Linux 7.6 64-bit	Intel® Xeon® E5-2600 v3 & v4	Cisco UCS B200 M4
Oracle Linux 7.6 64-bit	Intel® Xeon® Scalable Processors	Cisco UCS B200 M5
Oracle Linux 7.6 64-bit	Intel® Xeon® E5-2400/E5-2400 v2	Cisco UCS B22 M3
Oracle Linux 7.6 64-bit	Intel® Xeon® E7-2800/E7-8800	Cisco UCS B230 M2
Oracle Linux 7.6 64-bit	Intel® Xeon® E7-2800/E7-8800 v3	Cisco UCS B260 M4
Oracle Linux 7.6 64-bit	Intel® Xeon® E5-4600/E5-4600 v2	Cisco UCS B420 M3
Oracle Linux 7.6 64-bit	Intel® Xeon® E5-4600 v3 & v4	Cisco UCS B420 M4
Oracle Linux 7.6 64-bit	Intel® Xeon® E7-2800/E7-8800	Cisco UCS B440 M2
Oracle Linux 7.6 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 7.6 64-bit	Intel® Xeon® Scalable Processors	Cisco UCS B480 M5
Oracle Linux 7.6 64-bit	Intel® Xeon® E5-2400/E5-2400 v2	Cisco UCS C22 M3
Oracle Linux 7.6 64-bit	Intel® Xeon® E5-2600/E5-2600 v2	Cisco UCS C220 M3
Oracle Linux 7.6 64-bit	Intel® Xeon® E5-2600 v3 & v4	Cisco UCS C220 M4
Oracle Linux 7.6 64-bit	Intel® Xeon® Scalable Processors	Cisco UCS C220 M5
Oracle Linux 7.6 64-bit	Intel® Xeon® E5-2400/E5-2400 v2	Cisco UCS C24 M3
Oracle Linux 7.6 64-bit	Intel® Xeon® E5-2600/E5-2600 v2	Cisco UCS C240 M3
Oracle Linux 7.6 64-bit	Intel® Xeon® E5-2600 v3 & v4	Cisco UCS C240 M4
Oracle Linux 7.6 64-bit	Intel® Xeon® Scalable Processors	Cisco UCS C240 M5
Oracle Linux 7.6 64-bit	Intel® Xeon® E7-2800 v2/E7-4800 v2, v3 & v4/E7-8800 v2 & v4	Cisco UCS C460 M4
Oracle Linux 7.6 64-bit	Intel® Xeon® Scalable Processors	Cisco UCS C480 M5
Oracle Linux 7.6 64-bit	Intel® Xeon® D-1500	Cisco UCS E1120D-M3/K9



Operating Environment	Processor	Hardware
Oracle Linux 7.6 64-bit	Intel® Xeon® D-1500	Cisco UCS E180D-M3/K9
Oracle Linux 7.6 64-bit	Intel® Xeon® E5-2600 v3	Dell PowerEdge FC630
Oracle Linux 7.6 64-bit	Intel® Xeon® E5-4600 v3	Dell PowerEdge FC830
Oracle Linux 7.6 64-bit	Intel® Xeon® E5-2600 v3	Dell PowerEdge M630 Blade
Oracle Linux 7.6 64-bit	Intel® Xeon® E5-4600 v4	Dell PowerEdge M830 Blade
Oracle Linux 7.6 64-bit	Intel® Xeon® E5-2600 v3	Dell PowerEdge R630
Oracle Linux 7.6 64-bit	Intel® Xeon® E5-2600 v3	Dell PowerEdge R730
Oracle Linux 7.6 64-bit	Intel® Xeon® E5-2600 v3	Dell PowerEdge R730xd
Oracle Linux 7.6 64-bit	Intel® Xeon® E7-4800 v4	Dell PowerEdge R930
Oracle Linux 7.6 64-bit	Intel® Xeon® E5-2600 v3	Dell PowerEdge T630
Oracle Linux 7.6 64-bit	Intel® Xeon® E7-4800 v2/E7-8800 v2	Fujitsu PRIMEQUEST 2400E
Oracle Linux 7.6 64-bit	Intel® Xeon® E7-8800 v3	Fujitsu PRIMEQUEST 2400E2
Oracle Linux 7.6 64-bit	Intel® Xeon® E7-8800 v4	Fujitsu PRIMEQUEST 2400E3
Oracle Linux 7.6 64-bit	Intel® Xeon® E7-4800 v2	Fujitsu PRIMEQUEST2400L
Oracle Linux 7.6 64-bit	Intel® Xeon® E7-8800 v3	Fujitsu PRIMEQUEST2400L2
Oracle Linux 7.6 64-bit	Intel® Xeon® E7-8800 v4	Fujitsu PRIMEQUEST 2400L3
Oracle Linux 7.6 64-bit	Intel® Xeon® E7-4800 v2	Fujitsu PRIMEQUEST 2400S
Oracle Linux 7.6 64-bit	Intel® Xeon® E7-4800 v2	Fujitsu PRIMEQUEST 2400S Lite
Oracle Linux 7.6 64-bit	Intel® Xeon® E7-8800 v3	Fujitsu PRIMEQUEST 2400S2
Oracle Linux 7.6 64-bit	Intel® Xeon® E7-8800 v3	Fujitsu PRIMEQUEST 2400S2 Lite
Oracle Linux 7.6 64-bit	Intel® Xeon® E7-8800 v4	Fujitsu PRIMEQUEST 2400S3
Oracle Linux 7.6 64-bit	Intel® Xeon® E7-8800 v4	Fujitsu PRIMEQUEST 2400S3 Lite
Oracle Linux 7.6 64-bit	Intel® Xeon® E7-8800 v2	Fujitsu PRIMEQUEST 2800B
Oracle Linux 7.6 64-bit	Intel® Xeon® E7-8800 v3	Fujitsu PRIMEQUEST 2800B2
Oracle Linux 7.6 64-bit	Intel® Xeon® E7-8800 v4	Fujitsu PRIMEQUEST 2800B3
Oracle Linux 7.6 64-bit	Intel® Xeon® E7-8800 v2	Fujitsu PRIMEQUEST 2800E
Oracle Linux 7.6 64-bit	Intel® Xeon® E7-8800 v3	Fujitsu PRIMEQUEST 2800E2
Oracle Linux 7.6 64-bit	Intel® Xeon® E7-8800 v4	Fujitsu PRIMEQUEST 2800E3
Oracle Linux 7.6 64-bit	Intel® Xeon® E7-8800 v2	Fujitsu PRIMEQUEST 2800L
Oracle Linux 7.6 64-bit	Intel® Xeon® E7-8800 v3	Fujitsu PRIMEQUEST 2800L2
Oracle Linux 7.6 64-bit	Intel® Xeon® E7-8800 v4	Fujitsu PRIMEQUEST 2800L3
Oracle Linux 7.6 64-bit	Intel® Xeon® Scalable Processors	Fujitsu PRIMEQUEST 3800B
Oracle Linux 7.6 64-bit	Intel® Xeon® E5-2600 v3	Fujitsu PRIMERGY BX2580 M1
Oracle Linux 7.6 64-bit	Intel® Xeon® E5-2600 v4	Fujitsu PRIMERGY BX2580 M2
Oracle Linux 7.6 64-bit	Intel® Xeon® E5-2600 v3	Fujitsu PRIMERGY RX2530 M1
Oracle Linux 7.6 64-bit	Intel® Xeon® E5-2600 v4	Fujitsu PRIMERGY RX2530 M2
Oracle Linux 7.6 64-bit	Intel® Xeon® Scalable Processors	Fujitsu PRIMERGY RX2530 M4
Oracle Linux 7.6 64-bit	Intel® Xeon® E5-2600 v3	Fujitsu PRIMERGY RX2540 M1
Oracle Linux 7.6 64-bit	Intel® Xeon® E5-2600 v4	Fujitsu PRIMERGY RX2540 M2
Oracle Linux 7.6 64-bit	Intel® Xeon® Scalable Processors	Fujitsu PRIMERGY RX2540 M4
Oracle Linux 7.6 64-bit	Intel® Xeon® E7-4800 v2/E7-8800 v2	Fujitsu PRIMERGY RX4770 M1

Operating Environment	Processor	Hardware
Oracle Linux 7.6 64-bit	Intel® Xeon® E7-4800 v3/E7-8800 v3	Fujitsu PRIMERGY RX4770 M2
Oracle Linux 7.6 64-bit	Intel® Xeon® E7-4800 v4/E7-8800 v4	Fujitsu PRIMERGY RX4770 M3
Oracle Linux 7.6 64-bit	Intel® Xeon® Scalable Processors	Fujitsu PRIMERGY RX4770 M4
Oracle Linux 7.6 64-bit	Intel® Xeon® E5-2600 v4	Hitachi Compute Blade 2500 CB520H B4
Oracle Linux 7.6 64-bit	Intel® Xeon® E7-8800 v2	Hitachi Compute Blade 2500 CB520X B2
Oracle Linux 7.6 64-bit	Intel® Xeon® E7-8800 v3	Hitachi Compute Blade 2500 CB520X B3
Oracle Linux 7.6 64-bit	Intel® Xeon® E5-2600 v4	Hitachi Compute Blade 500 CB520H B4
Oracle Linux 7.6 64-bit	Intel® Xeon® E7-8800 v2	Hitachi Compute Blade 500 CB520X B2
Oracle Linux 7.6 64-bit	Intel® Xeon® E5-2600 v4	Hitachi QuantaGrid D51B-2U
Oracle Linux 7.6 64-bit	Intel® Xeon® E5-2600 v3 & v4	Hitachi QuantaPlex T41S-2U
Oracle Linux 7.6 64-bit	Intel® Xeon® Scalable Processors	Hitachi Vantara Hitachi Advanced Server DS120
Oracle Linux 7.6 64-bit	Intel® Xeon® Scalable Processors	Hitachi Vantara Hitachi Advanced Server DS220
Oracle Linux 7.6 64-bit	Intel® Xeon® Scalable Processors	Hitachi Vantara Hitachi Advanced Server DS240
Oracle Linux 7.6 64-bit	Intel® Xeon® E7-4800 v4/E7-8800 v4	HPE Integrity MC990 X
Oracle Linux 7.6 64-bit	Intel® Xeon® E5-2600 v2	HPE ProLiant BL460c Gen8
Oracle Linux 7.6 64-bit	Intel® Xeon® E5-2600 v3	HPE ProLiant BL460c Gen9
Oracle Linux 7.6 64-bit	Intel® Xeon® E5-4600 v3	HPE ProLiant BL660c Gen9
Oracle Linux 7.6 64-bit	Intel® Xeon® E5-2600 v3 & v4	HPE ProLiant DL160 Gen9
Oracle Linux 7.6 64-bit	Intel® Xeon® E5-2600 v3 & v4	HPE ProLiant DL180 Gen9
Oracle Linux 7.6 64-bit	Intel® Pentium® G2120 & Intel® Xeon® E3-1200 v2	HPE ProLiant DL320e Gen8
Oracle Linux 7.6 64-bit	Intel® Pentium® G3200-series/G3420, Core i3-4100-series/Intel® Xeon® E3-12 v3	HPE ProLiant DL320e Gen8 v2
Oracle Linux 7.6 64-bit	Intel® Xeon® E5-2600 v3 & v4	HPE ProLiant DL360 Gen9
Oracle Linux 7.6 64-bit	Intel® Xeon® E5-2400/E5-2400 v2	HPE ProLiant DL360e Gen8
Oracle Linux 7.6 64-bit	Intel® Xeon® E5-2600 v3 & v4	HPE ProLiant DL360p Gen8
Oracle Linux 7.6 64-bit	Intel® Xeon® E5-2600 v3 & v4	HPE ProLiant DL380 Gen9
Oracle Linux 7.6 64-bit	Intel® Xeon® E5-2400/E5-2400 v2	HPE ProLiant DL380e Gen8
Oracle Linux 7.6 64-bit	Intel® Xeon® E5-4600/E5-4600 v2	HPE ProLiant DL560 Gen8
Oracle Linux 7.6 64-bit	Intel® Xeon® E5-4600 v3 & v4	HPE ProLiant DL560 Gen9
Oracle Linux 7.6 64-bit	Intel® Xeon® E7-4800 v2/E7-8800 v2	HPE ProLiant DL580 Gen8
Oracle Linux 7.6 64-bit	Intel® Xeon® E7-4800 v3/E7-8800 v3	HPE ProLiant DL580 Gen9
Oracle Linux 7.6 64-bit	Intel® Xeon® E5-2600 v3 & v4	HPE ProLiant ML350 Gen9
Oracle Linux 7.6 64-bit	Intel® Xeon® E5-2600 v4	HPE Synergy 480 Gen9 Compute Module
Oracle Linux 7.6 64-bit	Intel® Xeon® E7-4800 v4/E7-8800 v4	HPE Synergy 620 Gen9 Compute Module
Oracle Linux 7.6 64-bit	Intel® Xeon® E7-4800 v4/E7-8800 v4	HPE Synergy 680 Gen9 Compute Module

Operating Environment	Processor	Hardware
Oracle Linux 7.6 64-bit	Intel® Xeon® Scalable Processors	Huawei FusionServer 1288H V5
Oracle Linux 7.6 64-bit	Intel® Xeon® Scalable Processors	Huawei FusionServer 2288H V5
Oracle Linux 7.6 64-bit	Intel® Xeon® Scalable Processors	Huawei FusionServer CH121 V5
Oracle Linux 7.6 64-bit	Intel® Xeon® Scalable Processors	Huawei FusionServer CH121L V5
Oracle Linux 7.6 64-bit	Intel® Xeon® Scalable Processors	Huawei FusionServer CH242 V5
Oracle Linux 7.6 64-bit	Intel® Xeon® E5-2600 v3 & v4	Huawei FusionServer RH2288H V3
Oracle Linux 7.6 64-bit	Intel® Xeon® Scalable Processors	Huawei FusionServer XH321 V5
Oracle Linux 7.6 64-bit	Intel® Xeon® E5-2600 v3 & v4	Inspur Yingxin NF5170M4
Oracle Linux 7.6 64-bit	Intel® Xeon® E5-2600 v3	Inspur Yingxin NF5180M4
Oracle Linux 7.6 64-bit	Intel® Xeon® E5-2600 v3 & v4	Inspur Yingxin NF5240M4
Oracle Linux 7.6 64-bit	Intel® Xeon® E5-2600 v3 & v4	Inspur Yingxin NF5270M4
Oracle Linux 7.6 64-bit	Intel® Xeon® E5-2600 v3 & v4	Inspur Yingxin NF5280M4
Oracle Linux 7.6 64-bit	Intel® Xeon® E5-2600 v3 & v4	Inspur Yingxin NF5460M4
Oracle Linux 7.6 64-bit	Intel® Xeon® E7-4800 v3 & v4/E7-8800 v3 & v4	Inspur Yingxin NX8480M4
Oracle Linux 7.6 64-bit	Intel® Xeon® Scalable 8100/6100/5100/4100/3100 Processors	Lenovo ThinkSystem SD530
Oracle Linux 7.6 64-bit	Intel® Xeon® Scalable 8100/6100/5100/4100/3100 Processors	Lenovo ThinkSystem SN550
Oracle Linux 7.6 64-bit	Intel® Xeon® Scalable 8100/6100/5100 Processors	Lenovo ThinkSystem SN850
Oracle Linux 7.6 64-bit	Intel® Xeon® Scalable 8100/6100/5100 Processors	Lenovo ThinkSystem SR850
Oracle Linux 7.6 64-bit	Intel® Xeon® Scalable 8100/6100/5100 Processors	Lenovo ThinkSystem SR860
Oracle Linux 7.6 64-bit	Intel® Xeon® Scalable 8100/6100/5100 Processors	Lenovo ThinkSystem SR950
Oracle Linux 7.6 64-bit	Intel® Xeon® E7-4800 v4/E7-8800 v4	NEC Express 5800/A1040d
Oracle Linux 7.6 64-bit	Intel® Xeon® E7-4800 v4/E7-8800 v4	NEC Express 5800/A2010d
Oracle Linux 7.6 64-bit	Intel® Xeon® E7-4800 v4/E7-8800 v4	NEC Express 5800/A2020d
Oracle Linux 7.6 64-bit	Intel® Xeon® E7-4800 v4/E7-8800 v4	NEC Express 5800/A2040d
Oracle Linux 7.6 64-bit	Intel® Xeon® E7-4800 v4/E7-8800 v4	NEC NX7700x/A4010M-4
Oracle Linux 7.6 64-bit	Intel® Xeon® E7-4800 v4/E7-8800 v4	NEC NX7700x/A4012L-1
Oracle Linux 7.6 64-bit	Intel® Xeon® E7-8800/4800 v4	NEC NX7700x/A4012L-1D
Oracle Linux 7.6 64-bit	Intel® Xeon® E7-4800 v4/E7-8800 v4	NEC NX7700x/A4012L-2
Oracle Linux 7.6 64-bit	Intel® Xeon® E7-8800/4800 v4	NEC NX7700x/A4012L-2D
Oracle Linux 7.6 64-bit	Intel® Xeon® E7-4800 v3/E7-8800 v3	NEC NX7700x/A4012M-4
Oracle Linux 7.6 64-bit	Intel® Xeon® E5-2600 v3	Oracle Netra Server X5-2
Oracle Linux 7.6 64-bit	Intel® Xeon® E5-2600 v3	Oracle Server X5-2
Oracle Linux 7.6 64-bit	Intel® Xeon® E5-2600 v3	Oracle Server X5-2L
Oracle Linux 7.6 64-bit	Intel® Xeon® E7-8800 v3	Oracle Server X5-4
Oracle Linux 7.6 64-bit	Intel® Xeon® E7-8800 v3	Oracle ServerX5-8
Oracle Linux 7.6 64-bit	Intel® Xeon® E5-2600 v4	Oracle Server X6-2
Oracle Linux 7.6 64-bit	Intel® Xeon® E5-2600 v4	Oracle Server X6-2L
Oracle Linux 7.6 64-bit	Intel® Xeon® E5-2600 v4	Oracle Server X6-2M
Oracle Linux 7.6 64-bit	Intel® Xeon® Scalable 8100/6100/4100 Processors	Oracle Server X7-2
Oracle Linux 7.6 64-bit	Intel® Xeon® Scalable 8100/6100/4100 Processors	Oracle Server X7-2L
Oracle Linux 7.6 64-bit	Intel® Xeon® Scalable 8100/6100 Processors	Oracle Server X7-8

Operating Environment	Processor	Hardware
Oracle Linux 7.6 64-bit	Intel® Xeon® x7500-series	Oracle Sun Fire X4470
Oracle Linux 7.6 64-bit	Intel® Xeon® x7500-series	Oracle Sun Fire X4800
Oracle Linux 7.6 64-bit	Intel® Xeon® E7-8800	Oracle Sun Server X2-8
Oracle Linux 7.6 64-bit	Intel® Xeon® E7-4800	Oracle Sun Server X2-4
Oracle Linux 7.6 64-bit	Intel® Xeon® E5-2600	Oracle Sun Server X3-2
Oracle Linux 7.6 64-bit	Intel® Xeon® E5-2600	Oracle Sun Server X3-2L
Oracle Linux 7.6 64-bit	Intel® Xeon® E5-2600 v2	Oracle Sun Server X4-2
Oracle Linux 7.6 64-bit	Intel® Xeon® E5-2600 v2	Oracle Sun Server X4-2L
Oracle Linux 7.6 64-bit	Intel® Xeon® E7-8800 v2	Oracle Sun Server X4-4
Oracle Linux 7.6 64-bit	Intel® Xeon® E7-8800 v2	Oracle Sun Server X4-8
Oracle Linux 7.6 64-bit	Intel® Xeon® E7-8800 v3 & v4	SGI UV 300RL
Oracle Linux 7.6 64-bit	Intel® Xeon® E7-4800 v4/ E7-8800 v3 & v4	SGI UV 300
Oracle Linux 7.6 64-bit	AMD Opteron™ 6000	Sugon A840-G10
Oracle Linux 7.6 64-bit	Intel® Xeon® E5-2600 v3 & v4	Sugon CB50-G20
Oracle Linux 7.6 64-bit	AMD Opteron™ 6000	Sugon CB85-G10
Oracle Linux 7.6 64-bit	Intel® Xeon® E5-2600 v3 & v4	Sugon CB85-G10
Oracle Linux 7.6 64-bit	Intel® Xeon® E7-4800 v2	Sugon CB80-G20
Oracle Linux 7.6 64-bit	Intel Xeon E7-8800/4800-v3 Series	Sugon CB80-G25
Oracle Linux 7.6 64-bit	AMD Opteron™ 6300	Sugon CB85-G10
Oracle Linux 7.6 64-bit	Intel® Xeon® 6100, 5100, 4100, 3100	Sugon I420-G30
Oracle Linux 7.6 64-bit	Intel® Xeon® E5-2600 v3	Sugon I610-G20
Oracle Linux 7.6 64-bit	Intel® Xeon® E5-2600 v3	Sugon I620-G20
Oracle Linux 7.6 64-bit	Intel® Xeon® 8100	Sugon I620-G30
Oracle Linux 7.6 64-bit	Intel® Xeon® E7-4800 v3 & v4	Sugon I840-G20
Oracle Linux 7.6 64-bit	Intel® Xeon® E7-4800 v2	Sugon I840-G25
Oracle Linux 7.6 64-bit	Intel® Xeon® E7-4800 v2 & v3/E7-8800 v2 & v3	Sugon I980-G20
Oracle Linux 7.6 64-bit	Intel® Xeon® E5-2600 v3 & v4	Sugon TC4600T
Oracle Linux 7.6 64-bit	Intel® Xeon® E5-2600 v3 & v4	Supermicro SuperServer SYS-6018U-TR4T+

**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 Vendor Affirmed Environments

The operating system is restricted to a single operator (concurrent operators are explicitly excluded). The application that request cryptographic services is the single user of the module, even when the application is serving multiple clients.

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 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 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		Hash (SHS)	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		Key Wrapping	NIST SP 800-38F key wrapping with AES	AES 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 <sup>2</sup>	Error detection code using crc32c, crct10dif	None	N/A
X		Data compression <sup>1</sup>	Performs data compression using deflate, lz4, lz4hc, lzo, zlib	None	N/A

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

**Table 8: FIPS Approved Operator Services and Descriptions**

<sup>2</sup> 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	Access Type(s)
X		Symmetric Encryption/Decryption	Encrypts or decrypts using non-Approved algorithms	AES-XTS (192-bit key), DES,	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 hash functions from SHA-1 mb	None	N/A
X		Keyed Hash	HMAC Keys < 112 bits.	HMAC keys < 112 bits.	R, W, X
X		Hash	SHA-1 (multiple-buffer) hashing functions	None	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	The 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	The 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 Keys ( $\geq 112$ bits)	N/A	The Key is passed into the module via API input parameter	kernel memory	Automatically zeroized when freeing the cipher handle
HMAC Integrity Key	N/A Installed with the module	N/A	Plaintext as part of the hmacsha512 application	Zeroized in memory by hmacsha512

**Table 10: CSP Table**

### 8.1 Random Number Generation

The module employs the Deterministic Random Bit Generator (DRBG) based on [SP800-90A] for the random number generation. 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 Linux Random Number Generator (NDRNG) as the entropy source. The NDRNG collects entropy from multiple noise sources with the main source coming from RDRAND from the Intel processor. The NDRNG provides at least 128 bits of entropy to the DRBG during initialization (seed) and reseed (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].

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.



CAVEAT: The module generates random strings whose strengths are modified by available entropy.

## 8.2 Key Entry/Output

An authorized application as user (the User role) has access to all key data generated during the operation of the module. Moreover, the module does not support the output of intermediate key generation values during the key generation process. 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 RSA public key used for signature verification of the kernel loadable components is stored outside of the module's boundary, in a keyring file in `/proc/keys/`.

## 8.4 Key/CSP Zeroization

The application that uses the module is responsible for appropriate destruction and zeroization of the key material. The module 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.



## 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 Module and no crypto operations are possible. The only recovery is to reboot the module. See section 10.3 for details. No operator intervention is required during the running of the self-tests.

### 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.
AES-GCM	KAT, encryption and decryption are tested separately.
Triple-DES	KAT, encryption and decryption are tested separately.
SP 800-90A CTR_DRBG	KAT
SP 800-90A Hash_DRBG	KAT
SP 800-90A HMAC_DRBG	KAT
HMAC	(SHA-1, SHA-256, SHA-512) KAT
Module Integrity test	Performed by sha512hmac application with HMAC-SHA-512 provided by NSS
RSA Signature Verification <sup>3</sup>	Part of the integrity test (considered as a KAT)

**Table 11: Power-On Self-Tests**

#### 9.1.1 Integrity Tests

For the module Integrity test, HMAC SHA-512 provided by the NSS bound module is tested before the NSS module makes itself available to the sha512hmac application. In addition, if the Intel or AMD AES-NI support is present and the dracut-fps aesni RPM package (see section 3) is installed, the AES-NI implementation is self-tested with the same KAT vector as the other AES implementations.

An HMAC SHA-512 (provided by the NSS bound module) calculation is performed on the sha512hmac utility and static Linux kernel binary to verify their integrity. The Linux kernel crypto API kernel components, and any additional code components loaded into the Linux kernel are checked with the RSA signature verification implementation of the Linux kernel when loading them into the kernel to confirm their integrity.

<sup>3</sup> The RSA signature verification is only used as part of integrity test and is not available as a service from the module.



NOTE: The fact that the kernel integrity check passed, which requires the loading of sha512hmac with the self tests implies a successful execution of the integrity and self tests of sha512hmac (the HMAC is stored in /usr/lib/hmaccalc/sha512hmac.hmac).

With respect to the integrity check of kernel loadable components providing the cryptographic functionality, the fact that the self test of these cryptographic components are displayed implies that the integrity checks of each kernel component passed successfully.

## 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.
DRBG	DRBG health tests as specified in section 11.3 of NIST SP 800-90Ar1

**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 UEK 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.)

The bound NSS module, certificate [# 4586](#) must be installed and configured to operate in the FIPS 140-2 Approved mode as outlined in section 10 of the [Security Policy](#) document.

#### 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 RPM file [kernel-uek-4.14.35-1902.300.11.el7uek.x86\\_64.rpm](#)  
# yum install [kernel-uek-4.14.35-1902.300.11.el7uek.x86\\_64.rpm](#)
2. Insure that the system is registered with the unbreakable Linux Network (ULN) and that the OL7\_X86\_64\_latest channel is enabled  
# yum-config-manager --enable ol7\_latest
3. Install the dracut-fips package:  
# yum install dracut-fips
4. Install the dracut-fips-aesni package (if AES-NI is supported):  
To check if AES-NI is supported run:  
# grep aes /proc/cpuinfo  
If it is supported, run:  
# yum install dracut-fips-aesni
5. Recreate the INITRAMFS image:  
# dracut -f
6. Perform the following steps to configure the boot loader so that the system boots into FIPS mode:

- a) Identify the boot partition and the UUID of the partition. 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
```

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

```
# blkid /dev/sda1
```

```
/dev/sda1: UUID="6046308a-75fc-418e-b284-72d8bfad34ba" TYPE="xfs"
```

- b) As the root user, edit the `/etc/default/grub` file as follows:

- i. Add the `fips=1` option to the boot loader configuration.  

```
GRUB_CMDLINE_LINUX="vconsole.font=latarcyrheb-sun16  
rd.lvm.lv=ol/swap rd.lvm.lv=ol/root crashkernel=auto  
vconsole.keymap=uk rhgb quiet fips=1"
```
- ii. If the contents of /boot reside on a different partition to the root partition, you must use the `boot=UUID=boot_UUID` line to the boot loader configuration to specify the device that should be mounted onto /boot when the kernel loads.  

```
GRUB_CMDLINE_LINUX="vconsole.font=latarcyrheb-sun16  
rd.lvm.lv=ol/swap rd.lvm.lv=ol/root crashkernel=auto  
vconsole.keymap=uk rhgb quiet  
boot=UUID=6046308a-75fc-418e-b284-72d8bfad34ba fips=1"
```
- iii. Save the changes.

This is required for FIPS to perform kernel validation checks, where it verifies the kernel against the provided HMAC file in the /boot directory.

**Note:**

On systems that are configured to boot with UEFI, /boot/efi is located on a dedicated partition as this is formatted specifically to meet UEFI requirements. This does not automatically mean that /boot is located on a dedicated partition.

Only use the `boot=` parameter if /boot is located on a dedicated partition. If the parameter is specified incorrectly or points to a non-existent device, the system may not boot.

If the system is no longer able to boot, you can try to modify the kernel boot options in grub to specify an alternate device for the `boot=UUID=boot_UUID` parameter, or remove the parameter entirely.

## 7. Rebuild the GRUB configuration as follows:

On BIOS-based systems, run the following command:

```
# grub2-mkconfig -o /boot/grub2/grub.cfg
```

On UEFI-based systems, run the following command:

```
# grub2-mkconfig -o /boot/efi/EFI/oracle/grub.cfg
```

To ensure proper operation of the in-module integrity verification, prelinking must be disabled on all system files. By default, the prelink package is not installed on the system. However, if it is installed, disable prelinking on all libraries and binaries as follows:

Set `PRELINKING=no` in the `/etc/sysconfig/prelink` configuration file.

If the libraries were already prelinked, undo the prelink on all of the system files as follows:

```
# prelink -u -a
```

8. Reboot the system

9. Verify that FIPS Mode is enabled by running the command:

```
# cat /proc/sys/crypto/fips_enabled
```

The response should be “1”

The version of the RPM containing the validated Modules is the version listed in Section 3. The integrity of the RPM is automatically verified during the installation of the Modules and the Crypto Officer shall not install the RPM file if the RPM tool indicates an integrity error.

### 10.1.2 FIPS 140-2 and AES NI Support

According to the UEK FIPS 140-2 Security Policy, the UEK 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-*
# recreate the initramfs image
dracut -f
```

The changes come into effect during the next reboot.

## 10.2 User Guidance

CTR and RFC 3686 mode must only be used for IPsec. It must not be used otherwise.

When using the Module, the user shall utilize the Oracle Linux UEK 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 Oracle Linux UEK.

Only the cryptographic mechanisms provided with the Oracle Linux UEK 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 mode must only be used in conjunction with the IPSEC as defined in RFC 4106 and RFC 5282. The module implements RFC 7296 compliant IKEv2 to establish the shared secret SKEYSEED from which the AES GCM encryption keys are derived.

In case the module's power is lost and then restored, the key used for the AES GCM shall be redistributed.

When a GCM IV is used for decryption, the responsibility for the IV generation lies with the party that performs the AES-GCM encryption therefore there is no restriction on the IV generation.

The implementation of the management logic for the last 64 bits of the “nonce” (the IV in RFC 5282) inside the module shall ensure that when the IV in RFC 5282 exhausts the maximum number of possible values for a given security association (e.g., a 64-bit counter starting from 0 and increasing, when it reaches the maximum value of  $2^{64} - 1$ ), either party to the security association that encounters this condition triggers a rekeying with IKEv2 to establish a new encryption key for the security association – see RFC 7296.

### 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. It is the user's responsibility to make sure that the module complies with this requirement and that the module does not exceed this limit.

## 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 panic 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 be 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 ringbuffer (**dmesg**) output is:

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

Typical messages are similar to "alg: self-tests for hmac(sha1-generic) (hmac(sha1)) 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
CCCS	Canadian Centre for Cyber Security
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
LRNG	Linux Random Number Generator
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

**Table 13: Acronyms**

## References

The FIPS 140-2 standard, and information on the CMVP, can be found at <https://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/technetwork/server-storage/linux/technologies/uek-overview-2043074.html>

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
PKCS#1	RSA Laboratories	PKCS#1 v2.1: RSA Cryptographic Standard

**Table 14: References**