# Red Hat, Inc.

# Red Hat Enterprise Linux 9 Kernel Cryptographic API

## FIPS 140-3 Non-Proprietary Security Policy

Document Version: 1.1

Last Modified: 2026/07/27

Prepared by:

atsec information security corporation

4516 Seton Center Pkwy, Suite 250

Austin, TX 78759

www.atsec.com

# Table of Contents

# List of Tables



# List of Figures

# 1 General

## 1.1 Overview

This document is the non-proprietary FIPS 140-3 Security Policy for version 5.14.0-427.124.1.el9_4; 1.4.0-2.el9 of the Red Hat Enterprise Linux 9 Kernel Cryptographic API module. It contains the security rules under which the module must operate and describes how this module meets the requirements as specified in FIPS PUB 140-3 (Federal Information Processing Standards Publication 140-3) for an overall Security Level 1 module.

This Non-Proprietary Security Policy may be reproduced and distributed, but only whole and intact and including this notice. Other documentation is proprietary to their authors.

### 1.1.1 How this Security Policy was prepared

In preparing the Security Policy document, the laboratory formatted the vendor-supplied documentation for consolidation without altering the technical statements therein contained. The further refining of the Security Policy document was conducted iteratively throughout the conformance testing, wherein the Security Policy was submitted to the vendor, who would then edit, modify, and add technical contents. The vendor would also supply additional documentation, which the laboratory formatted into the existing Security Policy, and resubmitted to the vendor for their final editing.

## 1.2 Security Levels

| Section | Title | Security Level |
|---|---|---|
| 1 | General | 1 |
| 2 | Cryptographic module specification | 1 |
| 3 | Cryptographic module interfaces | 1 |
| 4 | Roles, services, and authentication | 1 |
| 5 | Software/Firmware security | 1 |
| 6 | Operational environment | 1 |
| 7 | Physical security | N/A |
| 8 | Non-invasive security | N/A |
| 9 | Sensitive security parameter management | 1 |
| 10 | Self-tests | 1 |

| Section | Title | Security Level |
|---|---|---|
| 11 | Life-cycle assurance | 1 |
| 12 | Mitigation of other attacks | N/A |
| | Overall Level | 1 |

Table 1: Security Levels

# 2 Cryptographic Module Specification

## 2.1 Description

**Purpose and Use:**

The Red Hat Enterprise Linux 9 Kernel Cryptographic API module (hereafter referred to as "the module") provides a C language application program interface (API) for use by other (kernel space and user space) processes that require cryptographic functionality. The module operates on a general-purpose computer as part of the Linux kernel. Its cryptographic functionality can be accessed using the Linux Kernel Crypto API.

**Module Type**: Software

**Module Embodiment:** Multi-Chip Standalone

**Cryptographic Boundary:**

The cryptographic boundary of the module is defined as the kernel binary and the kernel crypto object files, the libkcapi library, and the sha512hmac binary, which is used to verify the integrity of the software components. In addition, the cryptographic boundary contains the .hmac files which store the expected integrity values for each of the software components.

**Tested Operational Environment's Physical Perimeter (TOEPP):**

The TOEPP of the module is defined as the general-purpose computer on which the module is installed.

The PAA/PAI provided by the processor are located within the module's physical perimeter is outside of the module's cryptographic boundary.

The cryptographic boundary and TOEPP are schematically represented in Figure 1.

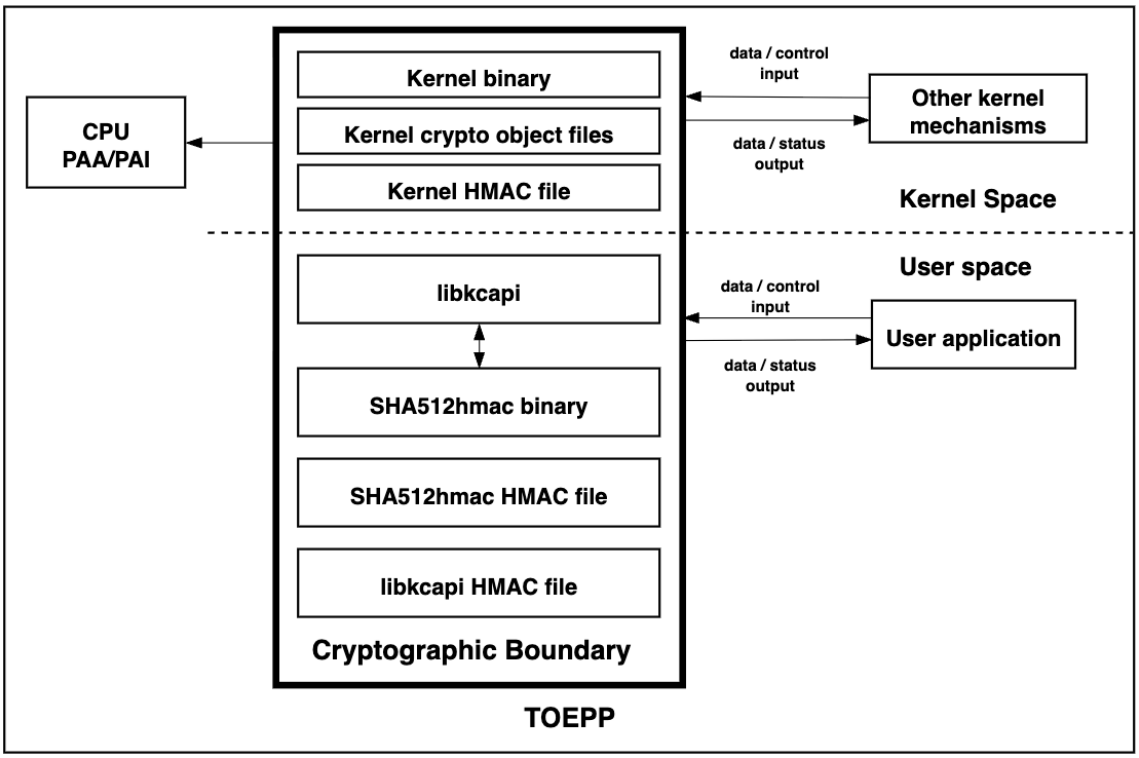


Figure 1: Block Diagram

## 2.2 Tested and Vendor Affirmed Module Version and Identification

**Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets):**

| Package or File Name | Software/ Firmware Version | Features | Integrity Test |
|---|---|---|---|
| /boot/vmlinuz-5.14.0-427.124.1.el9_4.x86_64; *.ko and *.ko.xz files in /usr/lib/modules/5.14.0-427.124.1.el9_4.x86_64/kernel/crypto; *.ko and *.ko.xz files in /usr/lib/modules/5.14.0-427.124.1.el9_4.x86_64/kernel/arch/x86/crypto *.ko; /usr/lib64/libkcapi.so.1.4.0, /usr/bin/sha512hmac | 5.14.0-427.124.1.el9_4; 1.4.0-2.el9-2.el9 | N/A | HMAC-SHA2-512 (vmlinuz, sha512hmac, libkcapi.so); RSA signature verification (*.ko.xz files) |

| Package or File Name | Software/ Firmware Version | Features | Integrity Test |
|---|---|---|---|
| /boot/vmlinuz-5.14.0-427.124.1.el9_4.s390x; *.ko and *.ko.xz files in /usr/lib/modules/5.14.0-427.124.1.el9_4.s390x/kernel/crypto; *.ko and *.ko.xz files in /usr/lib/modules/5.14.0-427.124.1.el9_4.s390x/kernel/arch/s390x/crypto *.ko; /usr/lib64/libkcapi.so.1.4.0, /usr/bin/sha512hmac | 5.14.0-427.124.1.el9_4; 1.4.0-2.el9 | N/A | HMAC-SHA2-512 (vmlinuz, sha512hmac, libkcapi.so); RSA signature verification (*.ko.xz files) |
| /boot/vmlinuz-5.14.0-427.124.1.el9_4.ppc64le; *.ko and *.ko.xz files in /usr/lib/modules/5.14.0-427.124.1.el9_4.ppc64le/kernel/crypto; *.ko and *.ko.xz files in /usr/lib/modules/5.14.0-427.124.1.el9_4.ppc64le/kernel/arch/ppc64le/crypto *.ko; /usr/lib64/libkcapi.so.1.4.0, /usr/bin/sha512hmac | 5.14.0-427.124.1.el9_4; 1.4.0-2.el9 | N/A | HMAC-SHA2-512 (vmlinuz, sha512hmac, libkcapi.so); RSA signature verification (*.ko.xz files) |

Table 2: Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets)

**Tested Operational Environments - Software, Firmware, Hybrid:**

| Operating System | Hardware Platform | Processors | PAA/PAI | Hypervisor or Host OS | Version(s) |
|---|---|---|---|---|---|
| Red Hat Enterprise Linux 9 | Dell PowerEdge R440 | Intel® Xeon® Silver 4216 | Yes | N/A | 5.14.0-427.124.1.el9_4; 1.4.0-2.el9 |
| Red Hat Enterprise Linux 9 | Dell PowerEdge R440 | Intel® Xeon® Silver 4216 | No | N/A | 5.14.0-427.124.1.el9_4; 1.4.0-2.el9 |
| Red Hat Enterprise Linux 9 | IBM z16 3931-A01 | IBM z16 | Yes | N/A | 5.14.0-427.124.1.el9_4; 1.4.0-2.el9 |
| Red Hat Enterprise Linux 9 | IBM z16 3931-A01 | IBM z16 | No | N/A | 5.14.0-427.124.1.el9_4; 1.4.0-2.el9 |

| Operating System | Hardware Platform | Processors | PAA/PAI | Hypervisor or Host OS | Version(s) |
|---|---|---|---|---|---|
| Red Hat Enterprise Linux 9 | IBM 9080-HEX | IBM POWER10 | Yes | PowerVM FW1040.00 with VIOS 3.1.3.00 | 5.14.0-427.124.1.el9_4; 1.4.0-2.el9 |
| Red Hat Enterprise Linux 9 | IBM 9080-HEX | IBM POWER10 | No | PowerVM FW1040.00 with VIOS 3.1.3.00 | 5.14.0-427.124.1.el9_4; 1.4.0-2.el9 |

Table 3: Tested Operational Environments - Software, Firmware, Hybrid

**Vendor-Affirmed Operational Environments - Software, Firmware, Hybrid:**

| Operating System | Hardware Platform |
|---|---|
| Red Hat Enterprise Linux 9 | Intel® Xeon® E5 |

Table 4: Vendor-Affirmed Operational Environments - Software, Firmware, Hybrid

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.

## 2.3 Excluded Components

There are no components within the cryptographic boundary excluded from the FIPS 140-3 requirements.

## 2.4 Modes of Operation

**Modes List and Description:**

| Mode Name | Description | Type | Status Indicator |
|---|---|---|---|
| Approved mode | Automatically entered whenever an approved service is requested | Approved | For all approved algorithms except AES GCM: respective approved service function returns indicator 0; For AES GCM: crypto_aead_get_flags(tfm) has the CRYPTO_TFM_FIPS_COMPLIANCE flag set |
| Non-approved mode | Automatically entered whenever a non-approved service is requested | Non-Approved | No service indicator required for non-approved services per IG 2.4.C |

Table 5: Modes List and Description

After passing all pre-operational self-tests and cryptographic algorithm self-tests executed on start-up, the module automatically transitions to the approved mode. No operator intervention is required to reach this point.

**Mode Change Instructions and Status:**

The module automatically switches between the approved and non-approved modes depending on the services requested by the operator. The status indicator of the mode of operation is equivalent to the indicator of the service that was requested.

## 2.5 Algorithms

**Approved Algorithms:**

| Algorithm | CAVP Cert | Properties | Reference |
|---|---|---|---|
| AES-CBC | A7145, A7153, A7156, A7371, A7374, A7420 | Direction - Decrypt, Encrypt<br>Key Length - 128, 192, 256 | SP 800-38A |
| AES-CBC-CS3 | A7150, A7161, A7378 | Direction - decrypt, encrypt<br>Key Length - 128, 192, 256 | SP 800-38A |
| AES-CCM | A7145, A7156, A7371, A7374 | Key Length - 128, 192, 256 | SP 800-38C |
| AES-CFB128 | A7148, A7159, A7370 | Direction - Decrypt, Encrypt<br>Key Length - 128, 192, 256 | SP 800-38A |
| AES-CMAC | A7145, A7156, A7371, A7374 | Direction - Generation, Verification<br>Key Length - 128, 192, 256 | SP 800-38B |
| AES-CTR | A7145, A7153, A7156, A7371, A7374, A7420 | Direction - Decrypt, Encrypt<br>Key Length - 128, 192, 256 | SP 800-38A |
| AES-ECB | A7145, A7151, A7152, A7153, A7154, A7155, A7156, A7157, A7158, A7371, A7372, A7373, A7374, A7375, A7376 | Direction - Decrypt, Encrypt<br>Key Length - 128, 192, 256 | SP 800-38A |
| AES-GCM | A7145, A7152, A7153, A7155, A7156, A7158, A7371, A7373, A7374, A7376 | Direction - Decrypt, Encrypt<br>IV Generation - External<br>Key Length - 128, 192, 256 | SP 800-38D |

| Algorithm | CAVP Cert | Properties | Reference |
|---|---|---|---|
| AES-GCM | A7151, A7154, A7157, A7372, A7375 | Direction - Encrypt<br>IV Generation - Internal<br>IV Generation Mode - 8.2.1<br>Key Length - 128, 192, 256 | SP 800-38D |
| AES-GMAC | A7145, A7156, A7371, A7374 | Direction - Decrypt, Encrypt<br>IV Generation - External<br>Key Length - 128, 192, 256 | SP 800-38D |
| AES-OFB | A7149, A7160, A7377 | Direction - Decrypt, Encrypt<br>Key Length - 128, 192, 256 | SP 800-38A |
| AES-XTS Testing Revision 2.0 | A7145, A7153, A7156, A7371, A7374, A7420 | Direction - Decrypt, Encrypt<br>Key Length - 128, 256 | SP 800-38E |
| Counter DRBG | A7145, A7151, A7152, A7153, A7154, A7155, A7156, A7157, A7158, A7371, A7372, A7373, A7374, A7375, A7376 | Prediction Resistance - No, Yes<br>Mode - AES-128, AES-192, AES-256<br>Derivation Function Enabled - Yes | SP 800-90A Rev. 1 |
| ECDSA SigVer (FIPS186-4) | A7146 | Component - No<br>Curve - P-256, P-384<br>Hash Algorithm - SHA-1 | FIPS 186-4 |
| ECDSA SigVer (FIPS186-5) | A7146 | Curve - P-256, P-384<br>Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512 | FIPS 186-5 |
| Hash DRBG | A7145, A7162, A7163, A7164, A7374 | Prediction Resistance - No, Yes<br>Mode - SHA-1, SHA2-256, SHA2-512 | SP 800-90A Rev. 1 |
| HMAC DRBG | A7145, A7162, A7163, A7164, A7374 | Prediction Resistance - No, Yes<br>Mode - SHA-1, SHA2-256, SHA2-512 | SP 800-90A Rev. 1 |
| HMAC-SHA-1 | A7145, A7162, A7163, A7164, A7374 | Key Length - Key Length: 112-524288 Increment 8 | FIPS 198-1 |

| Algorithm | CAVP Cert | Properties | Reference |
|---|---|---|---|
| HMAC-SHA2-224 | A7145, A7162, A7163, A7164, A7374 | Key Length - Key Length: 112-524288 Increment 8 | FIPS 198-1 |
| HMAC-SHA2-256 | A7145, A7162, A7163, A7164, A7374 | Key Length - Key Length: 112-524288 Increment 8 | FIPS 198-1 |
| HMAC-SHA2-384 | A7145, A7162, A7163, A7164, A7374 | Key Length - Key Length: 112-524288 Increment 8 | FIPS 198-1 |
| HMAC-SHA2-512 | A7145, A7162, A7163, A7164, A7374 | Key Length - Key Length: 112-524288 Increment 8 | FIPS 198-1 |
| HMAC-SHA3-224 | A7147, A7379 | Key Length - Key Length: 112-524288 Increment 8 | FIPS 198-1 |
| HMAC-SHA3-256 | A7147, A7379 | Key Length - Key Length: 112-524288 Increment 8 | FIPS 198-1 |
| HMAC-SHA3-384 | A7147, A7379 | Key Length - Key Length: 112-524288 Increment 8 | FIPS 198-1 |
| HMAC-SHA3-512 | A7147, A7379 | Key Length - Key Length: 112-524288 Increment 8 | FIPS 198-1 |
| KAS-FFC-SSC Sp800-56Ar3 | A7144 | Domain Parameter Generation Methods - ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192<br>Scheme -<br>dhEphem -<br>KAS Role - initiator, responder | SP 800-56A Rev. 3 |
| RSA SigVer (FIPS186-4) | A7145, A7162, A7163, A7164, A7374 | Signature Type - PKCS 1.5<br>Modulo - 2048, 3072, 4096 | FIPS 186-4 |
| RSA SigVer (FIPS186-5) | A7145, A7162, A7163, A7164, A7374 | Modulo - 2048, 3072, 4096<br>Signature Type - pkcs1v1.5 | FIPS 186-5 |
| Safe Primes Key Generation | A7144 | Safe Prime Groups - ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192 | SP 800-56A Rev. 3 |

| Algorithm | CAVP Cert | Properties | Reference |
|---|---|---|---|
| SHA-1 | A7145, A7162, A7163, A7164, A7374 | Message Length - Message Length: 0-65536 Increment 8<br>Large Message Sizes - 1, 2 | FIPS 180-4 |
| SHA2-224 | A7145, A7162, A7163, A7164, A7374 | Message Length - Message Length: 0-65536 Increment 8<br>Large Message Sizes - 1, 2 | FIPS 180-4 |
| SHA2-256 | A7145, A7162, A7163, A7164, A7374 | Message Length - Message Length: 0-65536 Increment 8<br>Large Message Sizes - 1, 2 | FIPS 180-4 |
| SHA2-384 | A7145, A7162, A7163, A7164, A7374 | Message Length - Message Length: 0-65536 Increment 8<br>Large Message Sizes - 1, 2 | FIPS 180-4 |
| SHA2-512 | A7145, A7162, A7163, A7164, A7374 | Message Length - Message Length: 0-65536 Increment 8<br>Large Message Sizes - 1, 2 | FIPS 180-4 |
| SHA3-224 | A7147, A7379 | Message Length - Message Length: 0-65536 Increment 8<br>Large Message Sizes - 1, 2 | FIPS 202 |
| SHA3-256 | A7147, A7379 | Message Length - Message Length: 0-65536 Increment 8<br>Large Message Sizes - 1, 2 | FIPS 202 |
| SHA3-384 | A7147, A7379 | Message Length - Message Length: 0-65536 Increment 8<br>Large Message Sizes - 1, 2 | FIPS 202 |
| SHA3-512 | A7147, A7379 | Message Length - Message Length: 0-65536 Increment 8<br>Large Message Sizes - 1, 2 | FIPS 202 |

Table 6: Approved Algorithms

**Vendor-Affirmed Algorithms:**

| Name | Properties | Implementation | Reference |
|---|---|---|---|
| Asymmetric Cryptographic Key Generation (CKG) | Key type:Asymmetric | N/A | SP 800-133 Rev. 2, section 4, example 1 |

Table 7: Vendor-Affirmed Algorithms

**Non-Approved, Allowed Algorithms:**

N/A for this module.

**Non-Approved, Allowed Algorithms with No Security Claimed:**

N/A for this module.

**Non-Approved, Not Allowed Algorithms:**

| Name | Use and Function |
|---|---|
| AES-GCM with external IV | Encryption with external IV (not compliant to FIPS 140-3 IG C.H) |
| KBKDF (libkcapi) | Key derivation with implementation not tested by CAVP |
| HKDF (libkcapi) | Key derivation with implementation not tested by CAVP |
| PBKDF2 (libkcapi) | Password-based key derivation with implementation not tested by CAVP |
| RSA | Encryption primitive; Decryption primitive (not compliant to SP 800-56Br2) |
| RSA with PKCS#1 v1.5 padding | Signature generation (pre-hashed message); Signature verification (pre-hashed message) |
| ECDSA | Signature generation (pre-hashed message); Signature verification (pre-hashed message) |

Table 8: Non-Approved, Not Allowed Algorithms

## 2.6 Security Function Implementations

| Name | Type | Description | Properties | Algorithms |
|---|---|---|---|---|
| Message digest | SHA | Compute a message digest | | SHA-1: (A7145, A7162, A7163, A7164, A7374) SHA2-224: (A7145, A7162, A7163, |

| Name | Type | Description | Properties | Algorithms |
|---|---|---|---|---|
| | | | | A7164, A7374)<br>SHA2-256: (A7145, A7162, A7163, A7164, A7374)<br>SHA2-384: (A7145, A7162, A7163, A7164, A7374)<br>SHA2-512: (A7145, A7162, A7163, A7164, A7374)<br>SHA3-224: (A7147, A7379)<br>SHA3-256: (A7147, A7379)<br>SHA3-384: (A7147, A7379)<br>SHA3-512: (A7147, A7379) |
| Encryption with AES | BC-UnAuth | Encrypt a plaintext with AES | | AES-CBC: (A7145, A7153, A7156, A7371, A7374, A7420)<br>AES-CBC-CS3: (A7150, A7161, A7378)<br>AES-CFB128: (A7148, A7159, A7370)<br>AES-CTR: (A7145, A7153, A7156, A7371, A7374, A7420)<br>AES-ECB: (A7145, A7151, A7152, A7153, A7154, A7155, A7156, A7157, A7158, A7371, A7372, A7373, A7374, A7375, A7376) |

| Name | Type | Description | Properties | Algorithms |
|---|---|---|---|---|
| | | | | AES-OFB: (A7149, A7160, A7377)<br>AES-XTS Testing Revision 2.0: (A7145, A7153, A7156, A7371, A7374, A7420) |
| Decryption with AES | BC-UnAuth | Decrypt a ciphertext with AES | | AES-CBC: (A7145, A7153, A7156, A7371, A7374, A7420)<br>AES-CBC-CS3: (A7150, A7161, A7378)<br>AES-CFB128: (A7148, A7159, A7370)<br>AES-CTR: (A7145, A7153, A7156, A7371, A7374, A7420)<br>AES-ECB: (A7145, A7151, A7152, A7153, A7154, A7155, A7156, A7157, A7158, A7371, A7372, A7373, A7374, A7375, A7376)<br>AES-OFB: (A7149, A7160, A7377)<br>AES-XTS Testing Revision 2.0: (A7145, A7153, A7156, A7371, A7374, A7420) |
| Authenticated encryption | BC-Auth | Encrypt and authenticate a plaintext | | AES-CCM: (A7145, A7156, A7371, A7374) |

| Name | Type | Description | Properties | Algorithms |
|---|---|---|---|---|
| | | | | AES-GCM: (A7145, A7151, A7152, A7153, A7154, A7155, A7156, A7157, A7158, A7371, A7372, A7373, A7374, A7375, A7376)<br>AES-CBC: (A7145, A7153, A7156, A7371, A7374, A7420)<br>AES-CTR: (A7145, A7153, A7156, A7371, A7374, A7420)<br>HMAC-SHA-1: (A7145, A7162, A7163, A7164, A7374)<br>HMAC-SHA2-224: (A7145, A7162, A7163, A7164, A7374)<br>HMAC-SHA2-256: (A7145, A7162, A7163, A7164, A7374)<br>HMAC-SHA2-384: (A7145, A7162, A7163, A7164, A7374)<br>HMAC-SHA2-512: (A7145, A7162, A7163, A7164, A7374) |
| Authenticated decryption | BC-Auth | Decrypt and authenticate a ciphertext | | AES-CCM: (A7145, A7156, A7371, A7374)<br>AES-GCM: (A7145, |

| Name | Type | Description | Properties | Algorithms |
|---|---|---|---|---|
| | | | | A7151, A7152, A7153, A7154, A7155, A7156, A7157, A7158, A7371, A7372, A7373, A7374, A7375, A7376)<br>AES-CBC: (A7145, A7153, A7156, A7371, A7374, A7420)<br>AES-CTR: (A7145, A7153, A7156, A7371, A7374, A7420)<br>HMAC-SHA-1: (A7145, A7162, A7163, A7164, A7374)<br>HMAC-SHA2-224: (A7145, A7162, A7163, A7164, A7374)<br>HMAC-SHA2-256: (A7145, A7162, A7163, A7164, A7374)<br>HMAC-SHA2-384: (A7145, A7162, A7163, A7164, A7374)<br>HMAC-SHA2-512: (A7145, A7162, A7163, A7164, A7374) |
| Message authentication | MAC | Compute a MAC tag for authentication | | AES-CMAC: (A7145, A7156, A7371, A7374)<br>AES-GMAC: (A7145, A7156, |

| Name | Type | Description | Properties | Algorithms |
|---|---|---|---|---|
| | | | | A7371, A7374)<br>HMAC-SHA-1: (A7145, A7162, A7163, A7164, A7374)<br>HMAC-SHA2-224: (A7145, A7162, A7163, A7164, A7374)<br>HMAC-SHA2-256: (A7145, A7162, A7163, A7164, A7374)<br>HMAC-SHA2-384: (A7145, A7162, A7163, A7164, A7374)<br>HMAC-SHA2-512: (A7145, A7162, A7163, A7164, A7374)<br>HMAC-SHA3-224: (A7147, A7379)<br>HMAC-SHA3-256: (A7147, A7379)<br>HMAC-SHA3-384: (A7147, A7379)<br>HMAC-SHA3-512: (A7147, A7379) |
| Random number generation with DRBGs | DRBG | Generate random numbers from DRBGs | | Counter DRBG: (A7145, A7151, A7152, A7153, A7154, A7155, A7156, A7157, A7158, A7371, A7372, A7373, A7374, A7375, A7376)<br>Hash DRBG: (A7145, A7162, |

| Name | Type | Description | Properties | Algorithms |
|---|---|---|---|---|
| | | | | A7163, A7164, A7374)<br>HMAC DRBG: (A7145, A7162, A7163, A7164, A7374) |
| Key pair generation with Safe Primes | AsymKeyPair-KeyGen<br>CKG | Generate an asymmetric DH key pair using Diffie-Hellman | | Safe Primes Key Generation: (A7144)<br>Asymmetric Cryptographic Key Generation (CKG): ()<br>Key type: Asymmetric |
| Digital signature verification with ECDSA | DigSig-SigVer | Digital signature verification using ECDSA with SHA2-224, SHA2-256, SHA2-384, SHA2-512 | | ECDSA SigVer (FIPS186-5): (A7146) |
| Digital signature verification with ECDSA (legacy use) | DigSig-SigVer | Digital signature verification using ECDSA with SHA-1 | Publications:FIPS 140-3 IG C.M legacy algorithms | ECDSA SigVer (FIPS186-4): (A7146) |
| Digital signature verification with RSA | DigSig-SigVer | PKCS 1.5 digital signature verification using RSA with SHA2-224, SHA2-256, SHA2-384, SHA2-512 | | RSA SigVer (FIPS186-5): (A7145, A7162, A7163, A7164, A7374) |
| Digital signature verification with RSA (legacy use) | DigSig-SigVer | PKCS 1.5 digital signature verification using RSA with SHA-1 | Publications:FIPS 140-3 IG C.M legacy algorithms | RSA SigVer (FIPS186-4): (A7145, A7162, |

| Name | Type | Description | Properties | Algorithms |
|---|---|---|---|---|
| | | | | A7163, A7164, A7374) |
| Shared secret computation with DH | KAS-SSC | Compute a shared secret using Diffie-Hellman | | KAS-FFC-SSC Sp800-56Ar3: (A7144) |

Table 9: Security Function Implementations

## 2.7 Algorithm Specific Information

### 2.7.1 AES GCM IV

The Crypto Officer shall consider the following requirements and restrictions when using the module.

For IPsec, the module offers the AES GCM implementation and uses the context of Scenario 1 of FIPS 140-3 IG C.H. The mechanism for IV generation is compliant with RFC 4106. IVs generated using this mechanism may only be used in the context of AES GCM encryption within the IPsec protocol.

The module does not implement IPsec. The module's implementation of AES GCM is used together with an application that runs outside the module's cryptographic boundary. This application must use RFC 7296 compliant IKEv2 to establish the shared secret SKEYSEED from which the AES GCM encryption keys are derived.

The design of the IPsec protocol implicitly ensures that the counter (the nonce_explicit part of the IV) does not exhaust the maximum number of possible values for a given session key.

In the event the module's power is lost and restored, the consuming application must ensure that a new key for use with the AES GCM key encryption or decryption under this scenario shall be established.

The module also provides a non-approved AES GCM encryption service which accepts arbitrary external IVs from the operator. This service can be requested by invoking the crypto_aead_encrypt API function with an AES GCM handle. When this is the case, the API will not set an approved service indicator, as described in section 4.3.

### 2.7.2 AES XTS

The length of a single data unit encrypted or decrypted with AES XTS shall not exceed $2^{20}$ AES blocks, that is 16MB, of data per XTS instance. An XTS instance is defined in Section 4 of SP 800-38E.

To meet the requirement stated in IG C.I, the module implements a check to ensure that the two AES keys used in AES XTS mode are not identical. As the module does not implement symmetric key generation, this check is performed when the keys are input by the operator. Key_1 and Key_2 shall be generated and/or established independently according to the rules for component symmetric keys from NIST SP 800-133r2, Section 6.3.

The XTS mode shall only be used for the cryptographic protection of data on storage devices. It shall not be used for other purposes, such as the encryption of data in transit.

### 2.7.3 RSA

For RSA signature verification, the module supports modulus size 3072 bits. The supported modulus size has been CAVP tested.

### 2.7.4 SP 800-56A Rev. 3 Assurances

To comply with the assurances found in Section 5.6.2 of SP 800-56A Rev. 3, the operator must use the Diffie-Hellman shared secret computation algorithms in the context of IETF protocols. Additionally, the module's approved key pair generation service (see Approved Services table in Section 4.3 Approved Services) must be used to generate ephemeral Diffie-Hellman key pairs, or the key pairs must be obtained from another FIPS-validated module. As part of this service, the module will internally perform the full public key validation of the generated public key.

The module's shared secret computation service will internally perform the full public key validation of the peer public key, complying with Section 5.6.2.2.2 of SP 800-56A Rev. 3.

### 2.7.5 Key Agreement

The module does not establish SSPs using an approved key agreement scheme (KAS). However, it does offer some or all of the underlying KAS cryptographic functionality to be used by an external operator/application as part of an approved KAS (e.g., KAS-FFC-SSC).

### 2.7.6 Legacy Use

RSA Digital signature verification using SHA-1 is allowed for legacy use only. Algorithms designated as "Legacy" can only be used on data that was generated prior to the Legacy Date specified in FIPS 140-3 IG C.M.

### 2.7.7 SHA-1

Digital signature generation using SHA-1 is non-approved and not allowed in approved services.

## 2.8 RBG and Entropy

| Cert Number | Vendor Name |
|---|---|
| E54 | Red Hat, Inc. |

Table 10: Entropy Certificates

| Name | Type | Operational Environment | Sample Size | Entropy per Sample | Conditioning Component |
|---|---|---|---|---|---|
| RHEL Kernel CPU Time Jitter RNG | Non-Physical | Red Hat Enterprise Linux 9 on Dell PowerEdge R440 on Intel® Xeon® Silver 4216; RHEL 9 on IBM Z System | 64 bits | 59 bits | Linear-Feedback Shift Register (LFSR) |

| Name | Type | Operational Environment | Sample Size | Entropy per Sample | Conditioning Component |
|---|---|---|---|---|---|
| Entropy Source | | z16(TM); Red Hat Enterprise Linux 9 on PowerVM FW1040.00 with VIOS 3.1.3.00 on IBM POWER Series POWER10 | | | |

Table 11: Entropy Sources

The module implements three different Deterministic Random Bit Generator (DRBG) implementations based on SP 800-90Ar1: CTR_DRBG, Hash_DRBG, and HMAC_DRBG. Each of these DRBG implementations can be instantiated by the operator of the module. When instantiated, these DRBGs can be used to generate random numbers for external usage.

Additionally, the module employs a specific HMAC SHA-512 DRBG implementation for internal purposes (e.g. to generate initialization vectors). This DRBG is initially seeded with 384 output bits from the entropy source (354 bits of entropy) and reseeded with 256 output bits from the entropy source (236 bits of entropy).

Outputs of multiple GetEntropy() calls are concatenated to receive the requested entropy input length.

The operational environment on the ESV certificate is identical to the operating system described in this document, and the entropy source is implemented inside the cryptographic boundary. Thus, the module is compliant with scenario 1 of IG 9.3.A. There are no maintenance requirements for the entropy source.

## 2.9 Key Generation

The module implements asymmetric key pair generation compliant with SP 800-133 Rev. 2 as listed in the Security Function Implementations table in 2.6 Security Function Implementations.

When random values are required, they are obtained from the SP 800-90A Rev. 1 approved DRBG, compliant with Section 4 of SP 800-133 Rev. 2 (without XOR).

Intermediate key generation values are not output from the module and are explicitly zeroized after processing the service.

## 2.10 Key Establishment

The module implements shared secret computation methods as listed in the Security Function Implementations table in 2.6 Security Function Implementations.

## 2.11 Industry Protocols

AES GCM with internal IV generation in the approved mode is compliant with RFC 4106 and shall only be used in conjunction with the IPsec protocol. No parts of this protocol, other than the AES GCM implementation, have been tested by the CAVP and CMVP.

# 3 Cryptographic Module Interfaces

## 3.1 Ports and Interfaces

| Physical Port | Logical Interface(s) | Data That Passes |
|---|---|---|
| N/A | Data Input | API data input parameters, AF_ALG type sockets |
| N/A | Data Output | API output parameters, AF_ALG type sockets |
| N/A | Control Input | API function calls, API control input parameters, AF_ALG type sockets, kernel command line |
| N/A | Status Output | API return values, AF_ALG type sockets, kernel logs |

Table 12: Ports and Interfaces

The logical interfaces are the APIs through which the applications request services. These logical interfaces are logically separated from each other by the API design, AF_ALG type socket that allows the applications running in the user space to request cryptographic services from the module.

The module does not support a control output interface.

# 4 Roles, Services, and Authentication

## 4.1 Authentication Methods

N/A for this module.

The module does not implement authentication.

## 4.2 Roles

| Name | Type | Operator Type | Authentication Methods |
|---|---|---|---|
| Crypto Officer | Role | CO | None |

Table 13: Roles

No support is provided for multiple concurrent operators.

## 4.3 Approved Services

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| Message digest | Compute a message digest | crypto_shash_init returns 0 | Message | Digest value | Message digest | Crypto Officer |
| Encryption | Encrypt a plaintext | crypto_skcipher_setkey returns 0 | AES key, plaintext, IV (if required) | Ciphertext | Encryption with AES | Crypto Officer<br>- AES key: W,E |
| Decryption | Decrypt a ciphertext | crypto_skcipher_setkey returns 0 | AES key, ciphertext, IV (if required) | Plaintext | Decryption with AES | Crypto Officer<br>- AES key: W,E |
| Authenticated encryption | Encrypt and authenticate a plaintext using CCM or GCM | For all except AES GCM: crypto_aead_setkey returns 0; For AES GCM: crypto_aead_get_flags(tfm) has the CRYPTO_TFM_FIPS_COMPLIANCE flag set | AES key, plaintext, IV (CCM/GCM) | Ciphertext, MAC tag (CCM/GCM) | Authenticated encryption | Crypto Officer<br>- AES key: W,E<br>- GCM IV: G,E,R |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| Authenticated decryption | Encrypt and authenticate a ciphertext using CCM or GCM | For all except AES GCM: crypto_aead_setkey returns 0; For AES GCM: crypto_aead_get_flags(tfm) has the CRYPTO_TFM_FIPS_COMPLIANCE flag set | AES key, ciphertext, IV (CCM/GCM), MAC tag (CCM/GCM) | Plaintext or failure | Authenticated decryption | Crypto Officer<br>- AES key: W,E<br>- GCM IV: W,E |
| Encrypt then MAC | Encrypt plaintext with AES (CBC or CTR) and use HMAC authenticate it | crypto_shash_init returns 0 | AES key, HMAC key, plaintext | Ciphertext, MAC tag | Authenticated encryption | Crypto Officer<br>- AES key: W,E<br>- HMAC key: W,E |
| Decrypt then verify | Decrypt an authenticated a ciphertext using AES (CBC or CTR) and HMAC | crypto_shash_init returns 0 | AES key, HMAC key, ciphertext, MAC tag | Plaintext or failure | Authenticated decryption | Crypto Officer<br>- AES key: W,E<br>- HMAC key: W,E |
| Message authentication | Compute a MAC tag using AES-GMAC, AES-CMAC, or HMAC | crypto_shash_init returns 0 | AES key or HMAC key, message | MAC tag | Message authentication | Crypto Officer<br>- AES key: W,E<br>- HMAC key: W,E |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| Random number generation | Generate random bytes | crypto_rng_get_bytes returns 0 | Output length | Random bytes | Random number generation with DRBGs | Crypto Officer<br>- Entropy Input (IG D.L): G,E,Z<br>- CTR_DRBG seed (IG D.L): G,E,Z<br>- HMAC_DRBG seed (IG D.L): G,E,Z<br>- Hash_DRBG seed (IG D.L): G,E,Z<br>- CTR_DRBG Internal state (V, Key) (IG D.L): G,W,E<br>- HMAC_DRBG Internal state (V, Key) (IG D.L): G,W,E<br>- Hash_DRBG Internal state (V, C) |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| | | | | | | (IG D.L): G,W,E |
| Random number generation using entropy source | Generate entropy from a dedicated instance of Jitter RNG | crypto_rng_get_bytes returns 0 | Output length | Random bytes | None | Crypto Officer |
| Key pair generation with Safe Primes | Generate a key pair using safe primes | crypto_kpp_set_secret() and crypto_kpp_generate_public_key() return 0 | Group | DH key pair | Key pair generation with Safe Primes | Crypto Officer<br>- Module-generated DH private key: G,R<br>- Module-generated DH public key: G,R<br>- Intermediate key generation value: G,E,Z |
| Shared secret computation | Compute a shared secret using Diffie-Hellman | crypto_kpp_compute_shared_secret() returns 0 | Public key (peer), Private key | Shared secret | Shared secret computation with DH | Crypto Officer<br>- DH private key: W,E<br>- DH public key: W,E<br>- Shared secret: G,R |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| Error detection code | Compute an EDC (crc32, crc32c, crct10dif) | None | Message | EDC | None | Crypto Officer |
| Compression | Compress data (deflate, lz4, lz4hc, lzo, zlib-deflate, zstd) | None | Data | Compressed data | None | Crypto Officer |
| Generic system call | Use the kernel to perform various non-cryptographic operations | None | Identifier, various arguments | Various return values | None | Crypto Officer |
| Show version | Return the module name and version information | None | N/A | Module name and version | None | Crypto Officer |
| Show status | Return the module status | None | N/A | Module status | None | Crypto Officer |
| Self-test | Perform the CASTs and | None | N/A | Pass/fail | Encryption with AES Decryptio | Crypto Officer |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| | integrity tests | | | | n with AES Message digest Message authentication Random number generation with DRBGs Digital signature verification with RSA Digital signature verification with RSA (legacy use) Digital signature verification with ECDSA Digital signature verification with ECDSA (legacy use) Authenticated encryption Authentic | |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| | | | | | ated decryption Shared secret computation with DH | |
| Zeroization | Zeroize SSPs | None | Any SSP | N/A | None | Crypto Officer<br>- AES key: Z<br>- GCM IV: Z<br>- HMAC key: Z<br>- Entropy Input (IG D.L): Z<br>- CTR_DRBG seed (IG D.L): Z<br>- HMAC_DRBG seed (IG D.L): Z<br>- Hash_DRBG seed (IG D.L): Z<br>- CTR_DRBG Internal state (V, Key) (IG D.L): Z<br>- HMAC_DRBG |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| | | | | | | Internal state (V, Key) (IG D.L): Z<br>- Hash_DRBG Internal state (V, C) (IG D.L): Z<br>- Intermediate key generation value: Z<br>- Module-generated DH private key: Z<br>- Module-generated DH public key: Z<br>- DH private key: Z<br>- DH public key: Z<br>- Shared secret: Z |

Table 14: Approved Services

The table above lists the approved services. The following convention is used to specify access rights to SSPs:

- **Generate (G):** The module generates or derives the SSP.
- **Read (R):** The SSP is read from the module (e.g. the SSP is output).
- **Write (W):** The SSP is updated, imported, or written to the module.
- **Execute (E):** The module uses the SSP in performing a cryptographic operation.
- **Zeroize (Z):** The module zeroizes the SSP.

## 4.4 Non-Approved Services

| Name | Description | Algorithms | Role |
|---|---|---|---|
| AES-GCM with external IV | Encrypt and authenticate a plaintext using AES-GCM with an external IV | AES-GCM with external IV | CO |
| Key derivation | Derive a key from a key-derivation key, a shared secret, or password | KBKDF (libkcapi)<br>HKDF (libkcapi)<br>PBKDF2 (libkcapi) | CO |
| Pre-hashed message signature generation | Generate a digital signature for a pre-hashed message | RSA with PKCS#1 v1.5 padding<br>ECDSA | CO |
| Pre-hashed message signature verification | Verify a digital signature for a pre-hashed message | RSA with PKCS#1 v1.5 padding<br>ECDSA | CO |
| Encryption primitive | Compute the RSA encryption primitive | RSA | CO |
| Decryption primitive | Compute the RSA decryption primitive | RSA | CO |

Table 15: Non-Approved Services

## 4.5 External Software/Firmware Loaded

The module does not load external software or firmware.

# 5 Software/Firmware Security

## 5.1 Integrity Techniques

The static kernel binary is integrity tested using an HMAC SHA-512 calculation performed by the sha512hmac utility (which utilizes the module's HMAC and SHA-512 implementations). The sha512hmac utility first executes the HMAC-SHA2-256 self-test. After this self-test is successful, the sha512hmac utility is used to perform an HMAC calculation of the libkcapi library, the kernel binary, and of its own binary to verify their integrity.

After the integrity of these components has been verified, the self-test for the RSA signature verification implementation is run. Upon successful run of this self-test, the RSA signature verification implementation of the kernel (with PKCS#1 v1.5 padding, SHA-256, and a 3072-bit key) is used to verify the integrity of the crypto object files listed in section 2.2 and loaded at start-up.

## 5.2 Initiate on Demand

Integrity tests are performed as part of the pre-operational self-tests, which are executed when the module is initialized. The integrity tests can be invoked on demand by unloading and subsequently re-initializing the module, which will perform (among others) the software integrity tests.

# 6 Operational Environment

## 6.1 Operational Environment Type and Requirements

**Type of Operational Environment**: Modifiable

**How Requirements are Satisfied:**

The operating system provides process isolation and memory protection mechanisms that ensure appropriate separation for memory access among the processes on the system. Each process has control over its own data and uncontrolled access to the data of other processes is prevented.

## 6.2 Configuration Settings and Restrictions

The module shall be installed as stated in Section 11.1.

Instrumentation tools like the ptrace system call, gdb and strace, as well as other tracing mechanisms offered by the Linux environment such as ftrace or systemtap, shall not be used in the operational environments. The use of any of these tools implies that the cryptographic module is running in a non-validated operational environment.

## 6.3 Additional Information

The Red Hat Enterprise Linux operating system is used as the basis of other products which include but are not limited to:

- Red Hat Enterprise Linux CoreOS
- Red Hat Ansible Automation Platform
- Red Hat OpenStack Platform
- Red Hat OpenShift
- Red Hat Gluster Storage
- Red Hat Satellite

Compliance is maintained for these products whenever the binary is found unchanged.

# 7 Physical Security

The module is comprised of software only and therefore this section is not applicable.

# 8 Non-Invasive Security

This module does not implement any non-invasive security mechanism and therefore this section is not applicable.

# 9 Sensitive Security Parameters Management

## 9.1 Storage Areas

| Storage Area Name | Description | Persistence Type |
|---|---|---|
| RAM | Temporary storage for SSPs used by the module as part of service execution | Dynamic |

Table 16: Storage Areas

The module does not perform persistent storage of SSPs. The SSPs are temporarily stored in the RAM in plaintext form. SSPs are provided to the module by the calling process and are destroyed when released by the appropriate zeroization function calls.

## 9.2 SSP Input-Output Methods

| Name | From | To | Format Type | Distribution Type | Entry Type | SFI or Algorithm |
|---|---|---|---|---|---|---|
| API input parameters; AF_ALG_type sockets (input) | Operator calling application (TOEPP) | Cryptographic module | Plaintext | Manual | Electronic | |
| API output parameters; AF_ALG_type sockets (output) | Cryptographic module | Operator calling application (TOEPP), kernel space | Plaintext | Manual | Electronic | |

Table 17: SSP Input-Output Methods

## 9.3 SSP Zeroization Methods

| Zeroization Method | Description | Rationale | Operator Initiation |
|---|---|---|---|
| Automatic | Automatically zeroized by the module when no longer needed | Memory occupied by SSPs is overwritten with zeroes, which renders the SSP values irretrievable. | N/A |

| Zeroization Method | Description | Rationale | Operator Initiation |
|---|---|---|---|
| Free cipher handle | Zeroizes the SSPs contained within the cipher handle | Memory occupied by SSPs is overwritten with zeroes, which renders the SSP values irretrievable. The completion of the zeroization routine indicates that the zeroization procedure succeeded. | By calling the appropriate zeroization functions: AES key: crypto_free_skcipher and crypto_free_aead; HMAC key: crypto_free_shash and crypto_free_ahash; DRBG internal state: crypto_free_rng; RSA public key, EC public key, DH public key: public_key_free; Shared secret: crypto_free_kpp |
| Remove power from the module | De-allocates the volatile memory used to store SSPs | Volatile memory used by the module is overwritten within nanoseconds when power is removed. Module power off indicates that the zeroization procedure succeeded. The successful removal of power implicitly indicates that the zeroization is complete. | By removing power |

Table 18: SSP Zeroization Methods

All data output is inhibited during zeroization.

## 9.4 SSPs

| Name | Description | Size - Strength | Type - Category | Generated By | Established By | Used By |
|---|---|---|---|---|---|---|
| AES key | AES key used for encryption, decryption, and computing MAC tags | 128, 192, 256 bits - 128, 192, 256 bits | Symmetric Key - CSP | | | Encryption with AES Decryption with AES Authenticated encryption Authenticated decryption Message authentication |

| Name | Description | Size - Strength | Type - Category | Generated By | Established By | Used By |
|---|---|---|---|---|---|---|
| GCM IV | AES GCM IV key used for authenticated encryption and decryption | 96 bits - N/A | IV - PSP | | | Authenticated encryption Authenticated decryption |
| HMAC key | HMAC key used for computing MAC tags | 112-524288 bits - 112-256 bits | Authentication key - CSP | | | Authenticated encryption Authenticated decryption Message authentication |
| Entropy Input (IG D.L) | Entropy input used to seed the DRBGs. Compliant with IG D.L. | 128-384 bits - 128-256 bits | Entropy input - CSP | | | Random number generation with DRBGs |
| CTR_DRBG seed (IG D.L) | CTR_DRBG seed derived from entropy input (IG D.L) | 256, 320, 384 bits - 128, 192, 256 bits | Seed - CSP | Random number generation with DRBGs | | Random number generation with DRBGs |
| HMAC_DRBG seed (IG D.L) | HMAC_DRBG seed derived from entropy input (IG D.L) | 160, 256, 512 bits - 128, 256 bits | Seed - CSP | Random number generation with DRBGs | | Random number generation with DRBGs |
| Hash_DRBG seed (IG D.L) | Hash_DRBG seed derived from entropy input (IG D.L) | 440, 888 bits - 128, 256 bits | Seed - CSP | Random number generation with DRBGs | | Random number generation with DRBGs |
| CTR_DRBG Internal state | Internal state of CTR_DRBG | 256, 320, 384 bits - | Internal state - CSP | Random number | | Random number |

| Name | Description | Size - Strength | Type - Category | Generated By | Established By | Used By |
|---|---|---|---|---|---|---|
| (V, Key) (IG D.L) | instances (IG D.L) | 128, 192, 256 bits | | generation with DRBGs | | generation with DRBGs |
| HMAC_DRBG Internal state (V, Key) (IG D.L) | Internal state of HMAC_DRBG instances (IG D.L) | 320, 512, 1024 bits - 128, 256 bits | Internal state - CSP | Random number generation with DRBGs | | Random number generation with DRBGs |
| Hash_DRBG Internal state (V, C) (IG D.L) | Internal state of Hash_DRBG instances (IG D.L) | 880, 1176 bits - 128, 256 bits | Internal state - CSP | Random number generation with DRBGs | | Random number generation with DRBGs |
| Intermediate key generation value | Intermediate key pair generation value generated during key generation services (SP 800-133 Rev. 2 Section 4, 5.1, and 5.2) | 112-8912 bits - 112-256 bits | Intermediate value - CSP | Key pair generation with Safe Primes | | Key pair generation with Safe Primes |
| Module-generated DH private key | DH private key generated by the module | ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192 - 112-200 bits | Private key - CSP | Key pair generation with Safe Primes | | Key pair generation with Safe Primes |
| Module-generated DH public key | DH public key generated by the module | ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, | Public key - PSP | Key pair generation with Safe Primes | | Key pair generation with Safe Primes |

| Name | Description | Size - Strength | Type - Category | Generated By | Established By | Used By |
|---|---|---|---|---|---|---|
| | | ffdhe8192 - 112-200 bits | | | | |
| DH private key | DH private key input to the module and used for shared secret computation | ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192 - 112-200 bits | Private key - CSP | | | Shared secret computation with DH |
| DH public key | DH public key input to the module and used for shared secret computation | ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192 - 112-200 bits | Public key - PSP | | | Shared secret computation with DH |
| Shared secret | Shared secret generated by ECDH/DH shared secret computation | 2048-8912 bits - 112-256 bits | Shared Secret - CSP | | Shared secret computation with DH | |

Table 19: SSP Table 1

| Name | Input - Output | Storage | Storage Duration | Zeroization | Related SSPs |
|---|---|---|---|---|---|
| AES key | API input parameters; AF_ALG_type sockets (input) | RAM:Plaintext | Until cipher handled is freed or module powered off | Free cipher handle Remove power from the module | |
| GCM IV | API input parameters; AF_ALG_type | RAM:Plaintext | Until cipher handled is freed or | Free cipher handle Remove | |

| Name | Input - Output | Storage | Storage Duration | Zeroization | Related SSPs |
|---|---|---|---|---|---|
| | sockets (input) API output parameters; AF_ALG_type sockets (output) | | module powered off | power from the module | |
| HMAC key | API input parameters; AF_ALG_type sockets (input) | RAM:Plaintext | Until cipher handled is freed or module powered off | Free cipher handle Remove power from the module | |
| Entropy Input (IG D.L) | | RAM:Plaintext | From generation until DRBG seed/reseed | Automatic | CTR_DRBG seed (IG D.L):Derives HMAC_DRBG seed (IG D.L):Derives Hash_DRBG seed (IG D.L):Derives |
| CTR_DRBG seed (IG D.L) | | RAM:Plaintext | While the DRBG is being instantiated | Automatic | Entropy Input (IG D.L):Derived From CTR_DRBG Internal state (V, Key) (IG D.L):Derives |
| HMAC_DRBG seed (IG D.L) | | RAM:Plaintext | While the DRBG is being instantiated | Automatic | Entropy Input (IG D.L):Derived From HMAC_DRBG Internal state (V, Key):Derives |
| Hash_DRBG seed (IG D.L) | | RAM:Plaintext | While the DRBG is being instantiated | Automatic | Entropy Input (IG D.L):Derived From Hash_DRBG Internal state (V, C) (IG D.L):Derives |

| Name | Input - Output | Storage | Storage Duration | Zeroization | Related SSPs |
|---|---|---|---|---|---|
| CTR_DRBG Internal state (V, Key) (IG D.L) | | RAM:Plaintext | From DRBG instantiation until DRBG termination | Free cipher handle Remove power from the module | CTR_DRBG seed (IG D.L):Derived From |
| HMAC_DRBG Internal state (V, Key) (IG D.L) | | RAM:Plaintext | From DRBG instantiation until DRBG termination | Free cipher handle Remove power from the module | HMAC_DRBG seed (IG D.L):Derived From |
| Hash_DRBG Internal state (V, C) (IG D.L) | | RAM:Plaintext | From DRBG instantiation until DRBG termination | Free cipher handle Remove power from the module | Hash_DRBG seed (IG D.L):Derived From |
| Intermediate key generation value | | RAM:Plaintext | From service invocation until it is completed | Automatic Remove power from the module | Module-generated DH private key:Generates Module-generated DH public key:Generates |
| Module-generated DH private key | API output parameters; AF_ALG_type sockets (output) | RAM:Plaintext | Until cipher handle is freed or module powered off | Free cipher handle Remove power from the module | Intermediate key generation value:Generated from Module-generated DH public key:Paired With |
| Module-generated DH public key | API output parameters; AF_ALG_type sockets (output) | RAM:Plaintext | Until cipher handle is freed or module powered off | Free cipher handle Remove power from the module | Intermediate key generation value:Generated from Module-generated DH private key:Paired With |

| Name | Input - Output | Storage | Storage Duration | Zeroization | Related SSPs |
|---|---|---|---|---|---|
| DH private key | API input parameters; AF_ALG_type sockets (input) | RAM:Plaintext | Until cipher handle is freed or module powered off | Free cipher handle Remove power from the module | DH public key:Paired With Shared secret:Establishes |
| DH public key | API input parameters; AF_ALG_type sockets (input) | RAM:Plaintext | Until cipher handle is freed or module powered off | Free cipher handle Remove power from the module | DH private key:Paired With Shared secret:Establishes |
| Shared secret | API output parameters; AF_ALG_type sockets (output) | RAM:Plaintext | From service invocation until cipherhandle is freed | Free cipher handle Remove power from the module | DH private key:Established By DH public key:Established By |

Table 20: SSP Table 2

## 9.5 Transitions

The SHA-1 algorithm as implemented by the module will be non-approved for all purposes except signature verification, starting January 1, 2031.

# 10 Self-Tests

## 10.1 Pre-Operational Self-Tests

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details |
|---|---|---|---|---|---|
| HMAC-SHA2-512 - sha512hmac | 128-bit key | Message Authentication | SW/FW Integrity | Module becomes operational and services are available for use. | Integrity test for sha512hmac binary |
| HMAC-SHA2-512 - libkcapi library | 128-bit key | Message Authentication | SW/FW Integrity | Module becomes operational and services are available for use. | Integrity test for libkcapi components |
| HMAC-SHA2-512 - vmlinuz | 128-bit key | Message Authentication | SW/FW Integrity | Module becomes operational and services are available for use. | Integrity test for vmlinuz binary |
| RSA SigVer (FIPS186-5) | 3072-bit key with SHA-256 | Signature Verification | SW/FW Integrity | Module becomes operational and services are available for use. | Integrity test for kernel object files |

Table 21: Pre-Operational Self-Tests

The pre-operational software integrity tests are performed automatically when the module is powered on, before the module transitions into the operational state. The algorithms used for the integrity test (i.e., HMAC-SHA2-512 and RSA SigVer with 3072-bit key) run their CASTs before the integrity test is performed. While the module is executing the self-tests, services are not available, and data output (via the data output interface) is inhibited until the pre-operational software integrity self-tests are successfully completed. The module transitions to the operational state only after the pre-operational self-tests are passed successfully.

## 10.2 Conditional Self-Tests

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| SHA-1 (A7145) | 0-8184 bit messages | KAT | CAST | Module becomes operational | Message digest | Module initialization |

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| | | | | and services are available for use. | | |
| SHA-1 (A7162) | 0-8184 bit messages | KAT | CAST | Module becomes operational and services are available for use. | Message digest | Module initialization |
| SHA-1 (A7163) | 0-8184 bit messages | KAT | CAST | Module becomes operational and services are available for use. | Message digest | Module initialization |
| SHA-1 (A7164) | 0-8184 bit messages | KAT | CAST | Module becomes operational and services are available for use. | Message digest | Module initialization |
| SHA-1 (A7374) | 0-8184 bit messages | KAT | CAST | Module becomes operational and services are available for use. | Message digest | Module initialization |
| SHA2-224 (A7145) | 0-8184 bit messages | KAT | CAST | Module becomes operational and services are available for use. | Message digest | Module initialization |

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| SHA2-224 (A7162) | 0-8184 bit messages | KAT | CAST | Module becomes operational and services are available for use. | Message digest | Module initialization |
| SHA2-224 (A7163) | 0-8184 bit messages | KAT | CAST | Module becomes operational and services are available for use. | Message digest | Module initialization |
| SHA2-224 (A7164) | 0-8184 bit messages | KAT | CAST | Module becomes operational and services are available for use. | Message digest | Module initialization |
| SHA2-224 (A7374) | 0-8184 bit messages | KAT | CAST | Module becomes operational and services are available for use. | Message digest | Module initialization |
| SHA2-256 (A7145) | 0-8184 bit messages | KAT | CAST | Module becomes operational and services are available for use. | Message digest | Module initialization |
| SHA2-256 (A7162) | 0-8184 bit messages | KAT | CAST | Module becomes operational and services | Message digest | Module initialization |

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| | | | | are available for use. | | |
| SHA2-256 (A7163) | 0-8184 bit messages | KAT | CAST | Module becomes operational and services are available for use. | Message digest | Module initialization |
| SHA2-256 (A7164) | 0-8184 bit messages | KAT | CAST | Module becomes operational and services are available for use. | Message digest | Module initialization |
| SHA2-256 (A7374) | 0-8184 bit messages | KAT | CAST | Module becomes operational and services are available for use. | Message digest | Module initialization |
| SHA2-384 (A7145) | 0-8184 bit messages | KAT | CAST | Module becomes operational and services are available for use. | Message digest | Module initialization |
| SHA2-384 (A7162) | 0-8184 bit messages | KAT | CAST | Module becomes operational and services are available for use. | Message digest | Module initialization |
| SHA2-384 (A7163) | 0-8184 bit messages | KAT | CAST | Module becomes operational | Message digest | Module initialization |

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| | | | | and services are available for use. | | |
| SHA2-384 (A7164) | 0-8184 bit messages | KAT | CAST | Module becomes operational and services are available for use. | Message digest | Module initialization |
| SHA2-384 (A7374) | 0-8184 bit messages | KAT | CAST | Module becomes operational and services are available for use. | Message digest | Module initialization |
| SHA2-512 (A7145) | 0-8184 bit messages | KAT | CAST | Module becomes operational and services are available for use. | Message digest | Module initialization |
| SHA2-512 (A7162) | 0-8184 bit messages | KAT | CAST | Module becomes operational and services are available for use. | Message digest | Module initialization |
| SHA2-512 (A7163) | 0-8184 bit messages | KAT | CAST | Module becomes operational and services are available for use. | Message digest | Module initialization |

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| SHA2-512 (A7164) | 0-8184 bit messages | KAT | CAST | Module becomes operational and services are available for use. | Message digest | Module initialization |
| SHA2-512 (A7374) | 0-8184 bit messages | KAT | CAST | Module becomes operational and services are available for use. | Message digest | Module initialization |
| SHA3-224 (A7147) | 0-8184 bit messages | KAT | CAST | Module becomes operational and services are available for use. | Message digest | Module initialization |
| SHA3-224 (A7379) | 0-8184 bit messages | KAT | CAST | Module becomes operational and services are available for use. | Message digest | Module initialization |
| SHA3-256 (A7147) | 0-8184 bit messages | KAT | CAST | Module becomes operational and services are available for use. | Message digest | Module initialization |
| SHA3-256 (A7379) | 0-8184 bit messages | KAT | CAST | Module becomes operational and services | Message digest | Module initialization |

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| | | | | are available for use. | | |
| SHA3-384 (A7147) | 0-8184 bit messages | KAT | CAST | Module becomes operational and services are available for use. | Message digest | Module initialization |
| SHA3-384 (A7379) | 0-8184 bit messages | KAT | CAST | Module becomes operational and services are available for use. | Message digest | Module initialization |
| SHA3-512 (A7147) | 0-8184 bit messages | KAT | CAST | Module becomes operational and services are available for use. | Message digest | Module initialization |
| SHA3-512 (A7379) | 0-8184 bit messages | KAT | CAST | Module becomes operational and services are available for use. | Message digest | Module initialization |
| AES-ECB - Encrypt (A7145) | 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| AES-ECB - Encrypt (A7151) | 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-ECB - Encrypt (A7152) | 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-ECB - Encrypt (A7153) | 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-ECB - Encrypt (A7154) | 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-ECB - Encrypt (A7155) | 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-ECB - Encrypt (A7156) | 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services | Encryption | Module initialization |

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| | | | | are available for use. | | |
| AES-ECB - Encrypt (A7157) | 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-ECB - Encrypt (A7158) | 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-ECB - Encrypt (A7371) | 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-ECB - Encrypt (A7372) | 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-ECB - Encrypt (A7373) | 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| AES-ECB - Encrypt (A7374) | 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-ECB - Encrypt (A7375) | 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-ECB - Encrypt (A7376) | 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-ECB - Decrypt (A7145) | 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| AES-ECB - Decrypt (A7151) | 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| AES-ECB - Decrypt (A7152) | 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services | Decryption | Module initialization |

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| | | | | are available for use. | | |
| AES-ECB - Decrypt (A7153) | 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| AES-ECB - Decrypt (A7154) | 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| AES-ECB - Decrypt (A7155) | 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| AES-ECB - Decrypt (A7156) | 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| AES-ECB - Decrypt (A7157) | 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| AES-ECB - Decrypt (A7158) | 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| AES-ECB - Decrypt (A7371) | 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| AES-ECB - Decrypt (A7372) | 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| AES-ECB - Decrypt (A7373) | 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| AES-ECB - Decrypt (A7374) | 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| AES-ECB - Decrypt (A7375) | 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services | Decryption | Module initialization |

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| | | | | are available for use. | | |
| AES-ECB - Decrypt (A7376) | 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| AES-CBC - Encrypt (A7145) | 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-CBC - Encrypt (A7153) | 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-CBC - Encrypt (A7156) | 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-CBC - Encrypt (A7371) | 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| AES-CBC - Encrypt (A7374) | 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-CBC - Encrypt (A7420) | 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-CBC - Decrypt (A7145) | 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| AES-CBC - Decrypt (A7153) | 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| AES-CBC - Decrypt (A7156) | 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| AES-CBC - Decrypt (A7371) | 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services | Decryption | Module initialization |

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| | | | | are available for use. | | |
| AES-CBC - Decrypt (A7374) | 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| AES-CBC - Decrypt (A7420) | 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| AES-CBC-CS3 - Encrypt (A7150) | 128 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-CBC-CS3 - Encrypt (A7161) | 128 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-CBC-CS3 - Encrypt (A7378) | 128 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-CBC-CS3 - | 128 bit keys | KAT | CAST | Module becomes operational | Decryption | Module initialization |

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| Decrypt (A7150) | | | | and services are available for use. | | |
| AES-CBC-CS3 - Decrypt (A7161) | 128 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| AES-CBC-CS3 - Decrypt (A7378) | 128 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| AES-OFB - Encrypt (A7149) | 128 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-OFB - Encrypt (A7160) | 128 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-OFB - Encrypt (A7377) | 128 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| AES-OFB - Decrypt (A7149) | 128 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| AES-OFB - Decrypt (A7160) | 128 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| AES-OFB - Decrypt (A7377) | 128 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| AES-CFB128 - Encrypt (A7148) | 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-CFB128 - Encrypt (A7159) | 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-CFB128 - Encrypt (A7370) | 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services | Encryption | Module initialization |

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| | | | | are available for use. | | |
| AES-CFB128 - Decrypt (A7148) | 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| AES-CFB128 - Decrypt (A7159) | 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| AES-CFB128 - Decrypt (A7370) | 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| AES-CTR - Encrypt (A7145) | 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-CTR - Encrypt (A7153) | 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| AES-CTR - Encrypt (A7156) | 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-CTR - Encrypt (A7371) | 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-CTR - Encrypt (A7374) | 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-CTR - Encrypt (A7420) | 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-CTR - Decrypt (A7145) | 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| AES-CTR - Decrypt (A7153) | 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services | Decryption | Module initialization |

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| | | | | are available for use. | | |
| AES-CTR - Decrypt (A7156) | 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| AES-CTR - Decrypt (A7371) | 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| AES-CTR - Decrypt (A7374) | 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| AES-CTR - Decrypt (A7420) | 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| AES-CCM - Encrypt (A7145) | 128, 192, 256 bit keys; 128-bit IVs | KAT | CAST | Module becomes operational and services are available for use. | Authenticated encryption | Module initialization |

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| AES-CCM - Encrypt (A7156) | 128, 192, 256 bit keys; 128-bit IVs | KAT | CAST | Module becomes operational and services are available for use. | Authenticated encryption | Module initialization |
| AES-CCM - Encrypt (A7371) | 128, 192, 256 bit keys; 128-bit IVs | KAT | CAST | Module becomes operational and services are available for use. | Authenticated encryption | Module initialization |
| AES-CCM - Encrypt (A7374) | 128, 192, 256 bit keys; 128-bit IVs | KAT | CAST | Module becomes operational and services are available for use. | Authenticated encryption | Module initialization |
| AES-CCM - Decrypt (A7145) | 128, 192, 256 bit keys; 128-bit IVs | KAT | CAST | Module becomes operational and services are available for use. | Authenticated decryption | Module initialization |
| AES-CCM - Decrypt (A7156) | 128, 192, 256 bit keys; 128-bit IVs | KAT | CAST | Module becomes operational and services are available for use. | Authenticated decryption | Module initialization |
| AES-CCM - Decrypt (A7371) | 128, 192, 256 bit keys; 128-bit IVs | KAT | CAST | Module becomes operational and services | Authenticated decryption | Module initialization |

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| | | | | are available for use. | | |
| AES-CCM - Decrypt (A7374) | 128, 192, 256 bit keys; 128-bit IVs | KAT | CAST | Module becomes operational and services are available for use. | Authenticated decryption | Module initialization |
| AES-GCM - Encrypt (A7145) | 128, 192, 256 bit keys and 96-bit IVs | KAT | CAST | Module becomes operational and services are available for use. | Authenticated encryption | Module initialization |
| AES-GCM - Encrypt (A7151) | 128, 192, 256 bit keys and 96-bit IVs | KAT | CAST | Module becomes operational and services are available for use. | Authenticated encryption | Module initialization |
| AES-GCM - Encrypt (A7152) | 128, 192, 256 bit keys and 96-bit IVs | KAT | CAST | Module becomes operational and services are available for use. | Authenticated encryption | Module initialization |
| AES-GCM - Encrypt (A7153) | 128, 192, 256 bit keys and 96-bit IVs | KAT | CAST | Module becomes operational and services are available for use. | Authenticated encryption | Module initialization |

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| AES-GCM - Encrypt (A7154) | 128, 192, 256 bit keys and 96-bit IVs | KAT | CAST | Module becomes operational and services are available for use. | Authenticated encryption | Module initialization |
| AES-GCM - Encrypt (A7155) | 128, 192, 256 bit keys and 96-bit IVs | KAT | CAST | Module becomes operational and services are available for use. | Authenticated encryption | Module initialization |
| AES-GCM - Encrypt (A7156) | 128, 192, 256 bit keys and 96-bit IVs | KAT | CAST | Module becomes operational and services are available for use. | Authenticated encryption | Module initialization |
| AES-GCM - Encrypt (A7157) | 128, 192, 256 bit keys and 96-bit IVs | KAT | CAST | Module becomes operational and services are available for use. | Authenticated encryption | Module initialization |
| AES-GCM - Encrypt (A7158) | 128, 192, 256 bit keys and 96-bit IVs | KAT | CAST | Module becomes operational and services are available for use. | Authenticated encryption | Module initialization |
| AES-GCM - Encrypt (A7371) | 128, 192, 256 bit keys and 96-bit IVs | KAT | CAST | Module becomes operational and services | Authenticated encryption | Module initialization |

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| | | | | are available for use. | | |
| AES-GCM - Encrypt (A7372) | 128, 192, 256 bit keys and 96-bit IVs | KAT | CAST | Module becomes operational and services are available for use. | Authenticated encryption | Module initialization |
| AES-GCM - Encrypt (A7373) | 128, 192, 256 bit keys and 96-bit IVs | KAT | CAST | Module becomes operational and services are available for use. | Authenticated encryption | Module initialization |
| AES-GCM - Encrypt (A7374) | 128, 192, 256 bit keys and 96-bit IVs | KAT | CAST | Module becomes operational and services are available for use. | Authenticated encryption | Module initialization |
| AES-GCM - Encrypt (A7375) | 128, 192, 256 bit keys and 96-bit IVs | KAT | CAST | Module becomes operational and services are available for use. | Authenticated encryption | Module initialization |
| AES-GCM - Encrypt (A7376) | 128, 192, 256 bit keys and 96-bit IVs | KAT | CAST | Module becomes operational and services are available for use. | Authenticated encryption | Module initialization |

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| AES-GCM - Decrypt (A7145) | 128, 192, 256 bit keys and 96-bit IVs | KAT | CAST | Module becomes operational and services are available for use. | Authenticated decryption | Module initialization |
| AES-GCM - Decrypt (A7151) | 128, 192, 256 bit keys and 96-bit IVs | KAT | CAST | Module becomes operational and services are available for use. | Authenticated decryption | Module initialization |
| AES-GCM - Decrypt (A7152) | 128, 192, 256 bit keys and 96-bit IVs | KAT | CAST | Module becomes operational and services are available for use. | Authenticated decryption | Module initialization |
| AES-GCM - Decrypt (A7153) | 128, 192, 256 bit keys and 96-bit IVs | KAT | CAST | Module becomes operational and services are available for use. | Authenticated decryption | Module initialization |
| AES-GCM - Decrypt (A7154) | 128, 192, 256 bit keys and 96-bit IVs | KAT | CAST | Module becomes operational and services are available for use. | Authenticated decryption | Module initialization |
| AES-GCM - Decrypt (A7155) | 128, 192, 256 bit keys and 96-bit IVs | KAT | CAST | Module becomes operational and services | Authenticated decryption | Module initialization |

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| | | | | are available for use. | | |
| AES-GCM - Decrypt (A7156) | 128, 192, 256 bit keys and 96-bit IVs | KAT | CAST | Module becomes operational and services are available for use. | Authenticated decryption | Module initialization |
| AES-GCM - Decrypt (A7157) | 128, 192, 256 bit keys and 96-bit IVs | KAT | CAST | Module becomes operational and services are available for use. | Authenticated decryption | Module initialization |
| AES-GCM - Decrypt (A7158) | 128, 192, 256 bit keys and 96-bit IVs | KAT | CAST | Module becomes operational and services are available for use. | Authenticated decryption | Module initialization |
| AES-GCM - Decrypt (A7371) | 128, 192, 256 bit keys and 96-bit IVs | KAT | CAST | Module becomes operational and services are available for use. | Authenticated decryption | Module initialization |
| AES-GCM - Decrypt (A7372) | 128, 192, 256 bit keys and 96-bit IVs | KAT | CAST | Module becomes operational and services are available for use. | Authenticated decryption | Module initialization |

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| AES-GCM - Decrypt (A7373) | 128, 192, 256 bit keys and 96-bit IVs | KAT | CAST | Module becomes operational and services are available for use. | Authenticated decryption | Module initialization |
| AES-GCM - Decrypt (A7374) | 128, 192, 256 bit keys and 96-bit IVs | KAT | CAST | Module becomes operational and services are available for use. | Authenticated decryption | Module initialization |
| AES-GCM - Decrypt (A7375) | 128, 192, 256 bit keys and 96-bit IVs | KAT | CAST | Module becomes operational and services are available for use. | Authenticated decryption | Module initialization |
| AES-GCM - Decrypt (A7376) | 128, 192, 256 bit keys and 96-bit IVs | KAT | CAST | Module becomes operational and services are available for use. | Authenticated decryption | Module initialization |
| AES-XTS Testing Revision 2.0 - Encrypt (A7145) | 128 and 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-XTS Testing Revision 2.0 - Encrypt (A7153) | 128 and 256 bit keys | KAT | CAST | Module becomes operational and services | Encryption | Module initialization |

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| | | | | are available for use. | | |
| AES-XTS Testing Revision 2.0 - Encrypt (A7156) | 128 and 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-XTS Testing Revision 2.0 - Encrypt (A7371) | 128 and 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-XTS Testing Revision 2.0 - Encrypt (A7374) | 128 and 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-XTS Testing Revision 2.0 - Encrypt (A7420) | 128 and 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-XTS Testing Revision 2.0 - Decrypt (A7145) | 128 and 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| AES-XTS Testing Revision 2.0 | 128 and 256 bit keys | KAT | CAST | Module becomes operational | Decryption | Module initialization |

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| - Decrypt (A7153) | | | | and services are available for use. | | |
| AES-XTS Testing Revision 2.0 - Decrypt (A7156) | 128 and 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| AES-XTS Testing Revision 2.0 - Decrypt (A7371) | 128 and 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| AES-XTS Testing Revision 2.0 - Decrypt (A7374) | 128 and 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| AES-XTS Testing Revision 2.0 - Decrypt (A7420) | 128 and 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| AES-CMAC (A7145) | 128 and 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Message authentication | Module initialization |

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| AES-CMAC (A7156) | 128 and 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Message authentication | Module initialization |
| AES-CMAC (A7371) | 128 and 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Message authentication | Module initialization |
| AES-CMAC (A7374) | 128 and 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Message authentication | Module initialization |
| HMAC-SHA-1 (A7145) | 32-64 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Message authentication | Module initialization |
| HMAC-SHA-1 (A7162) | 32-64 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Message authentication | Module initialization |
| HMAC-SHA-1 (A7163) | 32-64 bit keys | KAT | CAST | Module becomes operational and services | Message authentication | Module initialization |

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| | | | | are available for use. | | |
| HMAC-SHA-1 (A7164) | 32-64 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Message authentication | Module initialization |
| HMAC-SHA-1 (A7374) | 32-64 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Message authentication | Module initialization |
| HMAC-SHA2-224 (A7145) | 32-1048 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Message authentication | Module initialization |
| HMAC-SHA2-224 (A7162) | 32-1048 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Message authentication | Module initialization |
| HMAC-SHA2-224 (A7163) | 32-1048 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Message authentication | Module initialization |

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| HMAC-SHA2-224 (A7164) | 32-1048 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Message authentication | Module initialization |
| HMAC-SHA2-224 (A7374) | 32-1048 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Message authentication | Module initialization |
| HMAC-SHA2-256 (A7145) | 32-64 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Message authentication | Module initialization. Before integrity test. |
| HMAC-SHA2-256 (A7162) | 32-64 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Message authentication | Module initialization. Before integrity test. |
| HMAC-SHA2-256 (A7163) | 32-64 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Message authentication | Module initialization. Before integrity test. |
| HMAC-SHA2-256 (A7164) | 32-64 bit keys | KAT | CAST | Module becomes operational and services | Message authentication | Module initialization. Before integrity test. |

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| | | | | are available for use. | | |
| HMAC-SHA2-256 (A7374) | 32-64 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Message authentication | Module initialization. Before integrity test. |
| HMAC-SHA2-384 (A7145) | 32-1048 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Message authentication | Module initialization |
| HMAC-SHA2-384 (A7162) | 32-1048 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Message authentication | Module initialization |
| HMAC-SHA2-384 (A7163) | 32-1048 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Message authentication | Module initialization |
| HMAC-SHA2-384 (A7164) | 32-1048 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Message authentication | Module initialization |

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| HMAC-SHA2-384 (A7374) | 32-1048 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Message authentication | Module initialization |
| HMAC-SHA2-512 (A7145) | 32-1048 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Message authentication | Module initialization. Before integrity test. |
| HMAC-SHA2-512 (A7162) | 32-1048 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Message authentication | Module initialization. Before integrity test. |
| HMAC-SHA2-512 (A7163) | 32-1048 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Message authentication | Module initialization. Before integrity test. |
| HMAC-SHA2-512 (A7164) | 32-1048 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Message authentication | Module initialization. Before integrity test. |
| HMAC-SHA2-512 (A7374) | 32-1048 bit keys | KAT | CAST | Module becomes operational and services | Message authentication | Module initialization. Before integrity test. |

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| | | | | are available for use. | | |
| HMAC-SHA3-224 (A7147) | 32-1048 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Message authentication | Module initialization |
| HMAC-SHA3-224 (A7379) | 32-1048 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Message authentication | Module initialization |
| HMAC-SHA3-256 (A7147) | 32-1048 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Message authentication | Module initialization |
| HMAC-SHA3-256 (A7379) | 32-1048 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Message authentication | Module initialization |
| HMAC-SHA3-384 (A7147) | 32-1048 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Message authentication | Module initialization |

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| HMAC-SHA3-384 (A7379) | 32-1048 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Message authentication | Module initialization |
| HMAC-SHA3-512 (A7147) | 32-1048 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Message authentication | Module initialization |
| HMAC-SHA3-512 (A7379) | 32-1048 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Message authentication | Module initialization |
| Counter DRBG (A7145) | 128, 192, 256 bit keys with DF, with/without PR; Health test per section 11.3 of SP 800-90Arev1 | KAT | CAST | Module becomes operational and services are available for use. | SP 800-90A Rev. 1 (instantiate, reseed, generate) health test | Module initialization |
| Counter DRBG (A7151) | 128, 192, 256 bit keys with DF, with/without PR; Health test per section 11.3 of SP 800-90Arev1 | KAT | CAST | Module becomes operational and services are available for use. | SP 800-90A Rev. 1 (instantiate, reseed, generate) health test | Module initialization |
| Counter DRBG (A7152) | 128, 192, 256 bit keys with DF, with/without PR; Health test per | KAT | CAST | Module becomes operational and services | SP 800-90A Rev. 1 (instantiate, reseed, | Module initialization |

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| | section 11.3 of SP 800-90Arev1 | | | are available for use. | generate) health test | |
| Counter DRBG (A7153) | 128, 192, 256 bit keys with DF, with/without PR; Health test per section 11.3 of SP 800-90Arev1 | KAT | CAST | Module becomes operational and services are available for use. | SP 800-90A Rev. 1 (instantiate, reseed, generate) health test | Module initialization |
| Counter DRBG (A7154) | 128, 192, 256 bit keys with DF, with/without PR; Health test per section 11.3 of SP 800-90Arev1 | KAT | CAST | Module becomes operational and services are available for use. | SP 800-90A Rev. 1 (instantiate, reseed, generate) health test | Module initialization |
| Counter DRBG (A7155) | 128, 192, 256 bit keys with DF, with/without PR; Health test per section 11.3 of SP 800-90Arev1 | KAT | CAST | Module becomes operational and services are available for use. | SP 800-90A Rev. 1 (instantiate, reseed, generate) health test | Module initialization |
| Counter DRBG (A7156) | 128, 192, 256 bit keys with DF, with/without PR; Health test per section 11.3 of SP 800-90Arev1 | KAT | CAST | Module becomes operational and services are available for use. | SP 800-90A Rev. 1 (instantiate, reseed, generate) health test | Module initialization |
| Counter DRBG (A7157) | 128, 192, 256 bit keys with DF, with/without PR; Health test per section 11.3 of SP 800-90Arev1 | KAT | CAST | Module becomes operational and services are available for use. | SP 800-90A Rev. 1 (instantiate, reseed, generate) health test | Module initialization |

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| Counter DRBG (A7158) | 128, 192, 256 bit keys with DF, with/without PR; Health test per section 11.3 of SP 800-90Arev1 | KAT | CAST | Module becomes operational and services are available for use. | SP 800-90A Rev. 1 (instantiate, reseed, generate) health test | Module initialization |
| Counter DRBG (A7371) | 128, 192, 256 bit keys with DF, with/without PR; Health test per section 11.3 of SP 800-90Arev1 | KAT | CAST | Module becomes operational and services are available for use. | SP 800-90A Rev. 1 (instantiate, reseed, generate) health test | Module initialization |
| Counter DRBG (A7372) | 128, 192, 256 bit keys with DF, with/without PR; Health test per section 11.3 of SP 800-90Arev1 | KAT | CAST | Module becomes operational and services are available for use. | SP 800-90A Rev. 1 (instantiate, reseed, generate) health test | Module initialization |
| Counter DRBG (A7373) | 128, 192, 256 bit keys with DF, with/without PR; Health test per section 11.3 of SP 800-90Arev1 | KAT | CAST | Module becomes operational and services are available for use. | SP 800-90A Rev. 1 (instantiate, reseed, generate) health test | Module initialization |
| Counter DRBG (A7374) | 128, 192, 256 bit keys with DF, with/without PR; Health test per section 11.3 of SP 800-90Arev1 | KAT | CAST | Module becomes operational and services are available for use. | SP 800-90A Rev. 1 (instantiate, reseed, generate) health test | Module initialization |
| Counter DRBG (A7375) | 128, 192, 256 bit keys with DF, with/without PR; Health test per | KAT | CAST | Module becomes operational and services | SP 800-90A Rev. 1 (instantiate, reseed, | Module initialization |

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| | section 11.3 of SP 800-90Arev1 | | | are available for use. | generate) health test | |
| Counter DRBG (A7376) | 128, 192, 256 bit keys with DF, with/without PR; Health test per section 11.3 of SP 800-90Arev1 | KAT | CAST | Module becomes operational and services are available for use. | SP 800-90A Rev. 1 (instantiate, reseed, generate) health test | Module initialization |
| Hash DRBG (A7145) | SHA1, SHA2-256, SHA2-512 With/without PR; Health test per section 11.3 of SP 800-90Arev1 | KAT | CAST | Module becomes operational and services are available for use. | SP 800-90A Rev. 1 (instantiate, reseed, generate) health test | Module initialization |
| Hash DRBG (A7162) | SHA1, SHA2-256, SHA2-512 With/without PR; Health test per section 11.3 of SP 800-90Arev1 | KAT | CAST | Module becomes operational and services are available for use. | SP 800-90A Rev. 1 (instantiate, reseed, generate) health test | Module initialization |
| Hash DRBG (A7163) | SHA1, SHA2-256, SHA2-512 With/without PR; Health test per section 11.3 of SP 800-90Arev1 | KAT | CAST | Module becomes operational and services are available for use. | SP 800-90A Rev. 1 (instantiate, reseed, generate) health test | Module initialization |
| Hash DRBG (A7164) | SHA1, SHA2-256, SHA2-512 With/without PR; Health test per section 11.3 of SP 800-90Arev1 | KAT | CAST | Module becomes operational and services are available for use. | SP 800-90A Rev. 1 (instantiate, reseed, generate) health test | Module initialization |
| Hash DRBG (A7374) | SHA1, SHA2-256, SHA2-512 With/without PR; | KAT | CAST | Module becomes operational | SP 800-90A Rev. 1 (instantiate, | Module initialization |

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| | Health test per section 11.3 of SP 800-90Arev1 | | | and services are available for use. | reseed, generate) health test | |
| HMAC DRBG (A7145) | SHA1, SHA2-256, SHA2-512 With/without PR; Health test per section 11.3 of SP 800-90Arev1 | KAT | CAST | Module becomes operational and services are available for use. | SP 800-90A Rev. 1 (instantiate, reseed, generate) health test | Module initialization |
| HMAC DRBG (A7162) | SHA1, SHA2-256, SHA2-512 With/without PR; Health test per section 11.3 of SP 800-90Arev1 | KAT | CAST | Module becomes operational and services are available for use. | SP 800-90A Rev. 1 (instantiate, reseed, generate) health test | Module initialization |
| HMAC DRBG (A7163) | SHA1, SHA2-256, SHA2-512 With/without PR; Health test per section 11.3 of SP 800-90Arev1 | KAT | CAST | Module becomes operational and services are available for use. | SP 800-90A Rev. 1 (instantiate, reseed, generate) health test | Module initialization |
| HMAC DRBG (A7164) | SHA1, SHA2-256, SHA2-512 With/without PR; Health test per section 11.3 of SP 800-90Arev1 | KAT | CAST | Module becomes operational and services are available for use. | SP 800-90A Rev. 1 (instantiate, reseed, generate) health test | Module initialization |
| HMAC DRBG (A7374) | SHA1, SHA2-256, SHA2-512 With/without PR; Health test per section 11.3 of SP 800-90Arev1 | KAT | CAST | Module becomes operational and services are available for use. | SP 800-90A Rev. 1 (instantiate, reseed, generate) health test | Module initialization |

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| ECDSA SigVer (FIPS186-5) (A7146) | P-256 with SHA-256 | KAT | CAST | Module becomes operational and services are available for use. | Signature verification | Module initialization |
| RSA SigVer (FIPS186-5) (A7145) | 4096-bit key with SHA-256 | KAT | CAST | Module becomes operational and services are available for use. | Signature verification | Module initialization. Before integrity test. |
| RSA SigVer (FIPS186-5) (A7162) | 4096-bit key with SHA-256 | KAT | CAST | Module becomes operational and services are available for use. | Signature verification | Module initialization. Before integrity test. |
| RSA SigVer (FIPS186-5) (A7163) | 4096-bit key with SHA-256 | KAT | CAST | Module becomes operational and services are available for use. | Signature verification | Module initialization. Before integrity test. |
| RSA SigVer (FIPS186-5) (A7164) | 4096-bit key with SHA-256 | KAT | CAST | Module becomes operational and services are available for use. | Signature verification | Module initialization. Before integrity test. |
| RSA SigVer (FIPS186-5) (A7374) | 4096-bit key with SHA-256 | KAT | CAST | Module becomes operational and services | Signature verification | Module initialization. Before integrity test. |

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| | | | | are available for use. | | |
| KAS-FFC-SSC Sp800-56Ar3 (A7144) | ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, and ffdhe8192 | KAT | CAST | Module becomes operational and services are available for use. | Shared secret computation | Module initialization |
| Safe Primes Key Generation (A7144) | PCT according to Section 5.6.2.1.4 of SP 800-56A Rev. 3 | PCT | PCT | Module becomes operational and services are available for use. | Public key recomputation | During operational state of the module when the respective cryptographic functions are used. |
| Entropy Source - Init RCT | Cutoff C=61, 1024 samples. Repetition count test according to Section 4.4.1 of SP 800-90B | RCT | CAST | Module becomes operational and services are available for use. | Entropy source start-up test | Entropy source initialization |
| Entropy Source - Init APT | Cutoff C=355, window W=512, 1024 samples. Adaptive proportion test according to Section 4.4.2 of SP 800-90B | APT | CAST | Module becomes operational and services are available for use. | Entropy source start-up test | Entropy source initialization |
| Entropy Source - Continuous RCT | Intermittent cutoff C=31, permanent cutoff C=61. Repetition count test according to | RCT | CAST | Entropy source is operational and services | Entropy source continuous test | Continuously when the entropy source is accessed |

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| | Section 4.4.1 of SP 800-90B | | | are available for use. | | |
| Entropy Source - Continuous APT | Intermittent cutoff C=325, permanent cutoff C=255, window W=512. Adaptive proportion test according to Section 4.4.2 of SP 800-90B | APT | CAST | Entropy source is operational and services are available for use. | Entropy source continuous test | Continuously when the entropy source is accessed |

Table 22: Conditional Self-Tests

The module performs self-tests on all approved cryptographic algorithms as part of the approved services supported in the approved mode of operation, using the tests shown in the table above. Services are not available, and data output (via the data output interface) is inhibited during the conditional self-tests. If any of these tests fails, the module transitions to the Error State.

## 10.3 Periodic Self-Test Information

| Algorithm or Test | Test Method | Test Type | Period | Periodic Method |
|---|---|---|---|---|
| HMAC-SHA2-512 - sha512hmac | Message Authentication | SW/FW Integrity | On demand | Manually |
| HMAC-SHA2-512 - libkcapi library | Message Authentication | SW/FW Integrity | On demand | Manually |
| HMAC-SHA2-512 - vmlinuz | Message Authentication | SW/FW Integrity | On demand | Manually |
| RSA SigVer (FIPS186-5) | Signature Verification | SW/FW Integrity | On demand | Manually |

Table 23: Pre-Operational Periodic Information

| Algorithm or Test | Test Method | Test Type | Period | Periodic Method |
|---|---|---|---|---|
| SHA-1 (A7145) | KAT | CAST | On demand | Manually |

| Algorithm or Test | Test Method | Test Type | Period | Periodic Method |
|---|---|---|---|---|
| SHA-1 (A7162) | KAT | CAST | On demand | Manually |
| SHA-1 (A7163) | KAT | CAST | On demand | Manually |
| SHA-1 (A7164) | KAT | CAST | On demand | Manually |
| SHA-1 (A7374) | KAT | CAST | On demand | Manually |
| SHA2-224 (A7145) | KAT | CAST | On demand | Manually |
| SHA2-224 (A7162) | KAT | CAST | On demand | Manually |
| SHA2-224 (A7163) | KAT | CAST | On demand | Manually |
| SHA2-224 (A7164) | KAT | CAST | On demand | Manually |
| SHA2-224 (A7374) | KAT | CAST | On demand | Manually |
| SHA2-256 (A7145) | KAT | CAST | On demand | Manually |
| SHA2-256 (A7162) | KAT | CAST | On demand | Manually |
| SHA2-256 (A7163) | KAT | CAST | On demand | Manually |
| SHA2-256 (A7164) | KAT | CAST | On demand | Manually |
| SHA2-256 (A7374) | KAT | CAST | On demand | Manually |
| SHA2-384 (A7145) | KAT | CAST | On demand | Manually |
| SHA2-384 (A7162) | KAT | CAST | On demand | Manually |
| SHA2-384 (A7163) | KAT | CAST | On demand | Manually |
| SHA2-384 (A7164) | KAT | CAST | On demand | Manually |
| SHA2-384 (A7374) | KAT | CAST | On demand | Manually |
| SHA2-512 (A7145) | KAT | CAST | On demand | Manually |
| SHA2-512 (A7162) | KAT | CAST | On demand | Manually |

| Algorithm or Test | Test Method | Test Type | Period | Periodic Method |
|---|---|---|---|---|
| SHA2-512 (A7163) | KAT | CAST | On demand | Manually |
| SHA2-512 (A7164) | KAT | CAST | On demand | Manually |
| SHA2-512 (A7374) | KAT | CAST | On demand | Manually |
| SHA3-224 (A7147) | KAT | CAST | On demand | Manually |
| SHA3-224 (A7379) | KAT | CAST | On demand | Manually |
| SHA3-256 (A7147) | KAT | CAST | On demand | Manually |
| SHA3-256 (A7379) | KAT | CAST | On demand | Manually |
| SHA3-384 (A7147) | KAT | CAST | On demand | Manually |
| SHA3-384 (A7379) | KAT | CAST | On demand | Manually |
| SHA3-512 (A7147) | KAT | CAST | On demand | Manually |
| SHA3-512 (A7379) | KAT | CAST | On demand | Manually |
| AES-ECB - Encrypt (A7145) | KAT | CAST | On demand | Manually |
| AES-ECB - Encrypt (A7151) | KAT | CAST | On demand | Manually |
| AES-ECB - Encrypt (A7152) | KAT | CAST | On demand | Manually |
| AES-ECB - Encrypt (A7153) | KAT | CAST | On demand | Manually |
| AES-ECB - Encrypt (A7154) | KAT | CAST | On demand | Manually |
| AES-ECB - Encrypt (A7155) | KAT | CAST | On demand | Manually |

| Algorithm or Test | Test Method | Test Type | Period | Periodic Method |
|---|---|---|---|---|
| AES-ECB - Encrypt (A7156) | KAT | CAST | On demand | Manually |
| AES-ECB - Encrypt (A7157) | KAT | CAST | On demand | Manually |
| AES-ECB - Encrypt (A7158) | KAT | CAST | On demand | Manually |
| AES-ECB - Encrypt (A7371) | KAT | CAST | On demand | Manually |
| AES-ECB - Encrypt (A7372) | KAT | CAST | On demand | Manually |
| AES-ECB - Encrypt (A7373) | KAT | CAST | On demand | Manually |
| AES-ECB - Encrypt (A7374) | KAT | CAST | On demand | Manually |
| AES-ECB - Encrypt (A7375) | KAT | CAST | On demand | Manually |
| AES-ECB - Encrypt (A7376) | KAT | CAST | On demand | Manually |
| AES-ECB - Decrypt (A7145) | KAT | CAST | On demand | Manually |
| AES-ECB - Decrypt (A7151) | KAT | CAST | On demand | Manually |
| AES-ECB - Decrypt (A7152) | KAT | CAST | On demand | Manually |
| AES-ECB - Decrypt (A7153) | KAT | CAST | On demand | Manually |
| AES-ECB - Decrypt (A7154) | KAT | CAST | On demand | Manually |

| Algorithm or Test | Test Method | Test Type | Period | Periodic Method |
|---|---|---|---|---|
| AES-ECB - Decrypt (A7155) | KAT | CAST | On demand | Manually |
| AES-ECB - Decrypt (A7156) | KAT | CAST | On demand | Manually |
| AES-ECB - Decrypt (A7157) | KAT | CAST | On demand | Manually |
| AES-ECB - Decrypt (A7158) | KAT | CAST | On demand | Manually |
| AES-ECB - Decrypt (A7371) | KAT | CAST | On demand | Manually |
| AES-ECB - Decrypt (A7372) | KAT | CAST | On demand | Manually |
| AES-ECB - Decrypt (A7373) | KAT | CAST | On demand | Manually |
| AES-ECB - Decrypt (A7374) | KAT | CAST | On demand | Manually |
| AES-ECB - Decrypt (A7375) | KAT | CAST | On demand | Manually |
| AES-ECB - Decrypt (A7376) | KAT | CAST | On demand | Manually |
| AES-CBC - Encrypt (A7145) | KAT | CAST | On demand | Manually |
| AES-CBC - Encrypt (A7153) | KAT | CAST | On demand | Manually |
| AES-CBC - Encrypt (A7156) | KAT | CAST | On demand | Manually |
| AES-CBC - Encrypt (A7371) | KAT | CAST | On demand | Manually |

| Algorithm or Test | Test Method | Test Type | Period | Periodic Method |
|---|---|---|---|---|
| AES-CBC - Encrypt (A7374) | KAT | CAST | On demand | Manually |
| AES-CBC - Encrypt (A7420) | KAT | CAST | On demand | Manually |
| AES-CBC - Decrypt (A7145) | KAT | CAST | On demand | Manually |
| AES-CBC - Decrypt (A7153) | KAT | CAST | On demand | Manually |
| AES-CBC - Decrypt (A7156) | KAT | CAST | On demand | Manually |
| AES-CBC - Decrypt (A7371) | KAT | CAST | On demand | Manually |
| AES-CBC - Decrypt (A7374) | KAT | CAST | On demand | Manually |
| AES-CBC - Decrypt (A7420) | KAT | CAST | On demand | Manually |
| AES-CBC-CS3 - Encrypt (A7150) | KAT | CAST | On demand | Manually |
| AES-CBC-CS3 - Encrypt (A7161) | KAT | CAST | On demand | Manually |
| AES-CBC-CS3 - Encrypt (A7378) | KAT | CAST | On demand | Manually |
| AES-CBC-CS3 - Decrypt (A7150) | KAT | CAST | On demand | Manually |
| AES-CBC-CS3 - Decrypt (A7161) | KAT | CAST | On demand | Manually |
| AES-CBC-CS3 - Decrypt (A7378) | KAT | CAST | On demand | Manually |

| Algorithm or Test | Test Method | Test Type | Period | Periodic Method |
|---|---|---|---|---|
| AES-OFB - Encrypt (A7149) | KAT | CAST | On demand | Manually |
| AES-OFB - Encrypt (A7160) | KAT | CAST | On demand | Manually |
| AES-OFB - Encrypt (A7377) | KAT | CAST | On demand | Manually |
| AES-OFB - Decrypt (A7149) | KAT | CAST | On demand | Manually |
| AES-OFB - Decrypt (A7160) | KAT | CAST | On demand | Manually |
| AES-OFB - Decrypt (A7377) | KAT | CAST | On demand | Manually |
| AES-CFB128 - Encrypt (A7148) | KAT | CAST | On demand | Manually |
| AES-CFB128 - Encrypt (A7159) | KAT | CAST | On demand | Manually |
| AES-CFB128 - Encrypt (A7370) | KAT | CAST | On demand | Manually |
| AES-CFB128 - Decrypt (A7148) | KAT | CAST | On demand | Manually |
| AES-CFB128 - Decrypt (A7159) | KAT | CAST | On demand | Manually |
| AES-CFB128 - Decrypt (A7370) | KAT | CAST | On demand | Manually |
| AES-CTR - Encrypt (A7145) | KAT | CAST | On demand | Manually |
| AES-CTR - Encrypt (A7153) | KAT | CAST | On demand | Manually |

| Algorithm or Test | Test Method | Test Type | Period | Periodic Method |
|---|---|---|---|---|
| AES-CTR - Encrypt (A7156) | KAT | CAST | On demand | Manually |
| AES-CTR - Encrypt (A7371) | KAT | CAST | On demand | Manually |
| AES-CTR - Encrypt (A7374) | KAT | CAST | On demand | Manually |
| AES-CTR - Encrypt (A7420) | KAT | CAST | On demand | Manually |
| AES-CTR - Decrypt (A7145) | KAT | CAST | On demand | Manually |
| AES-CTR - Decrypt (A7153) | KAT | CAST | On demand | Manually |
| AES-CTR - Decrypt (A7156) | KAT | CAST | On demand | Manually |
| AES-CTR - Decrypt (A7371) | KAT | CAST | On demand | Manually |
| AES-CTR - Decrypt (A7374) | KAT | CAST | On demand | Manually |
| AES-CTR - Decrypt (A7420) | KAT | CAST | On demand | Manually |
| AES-CCM - Encrypt (A7145) | KAT | CAST | On demand | Manually |
| AES-CCM - Encrypt (A7156) | KAT | CAST | On demand | Manually |
| AES-CCM - Encrypt (A7371) | KAT | CAST | On demand | Manually |
| AES-CCM - Encrypt (A7374) | KAT | CAST | On demand | Manually |

| Algorithm or Test | Test Method | Test Type | Period | Periodic Method |
|---|---|---|---|---|
| AES-CCM - Decrypt (A7145) | KAT | CAST | On demand | Manually |
| AES-CCM - Decrypt (A7156) | KAT | CAST | On demand | Manually |
| AES-CCM - Decrypt (A7371) | KAT | CAST | On demand | Manually |
| AES-CCM - Decrypt (A7374) | KAT | CAST | On demand | Manually |
| AES-GCM - Encrypt (A7145) | KAT | CAST | On demand | Manually |
| AES-GCM - Encrypt (A7151) | KAT | CAST | On demand | Manually |
| AES-GCM - Encrypt (A7152) | KAT | CAST | On demand | Manually |
| AES-GCM - Encrypt (A7153) | KAT | CAST | On demand | Manually |
| AES-GCM - Encrypt (A7154) | KAT | CAST | On demand | Manually |
| AES-GCM - Encrypt (A7155) | KAT | CAST | On demand | Manually |
| AES-GCM - Encrypt (A7156) | KAT | CAST | On demand | Manually |
| AES-GCM - Encrypt (A7157) | KAT | CAST | On demand | Manually |
| AES-GCM - Encrypt (A7158) | KAT | CAST | On demand | Manually |
| AES-GCM - Encrypt (A7371) | KAT | CAST | On demand | Manually |

| Algorithm or Test | Test Method | Test Type | Period | Periodic Method |
|---|---|---|---|---|
| AES-GCM - Encrypt (A7372) | KAT | CAST | On demand | Manually |
| AES-GCM - Encrypt (A7373) | KAT | CAST | On demand | Manually |
| AES-GCM - Encrypt (A7374) | KAT | CAST | On demand | Manually |
| AES-GCM - Encrypt (A7375) | KAT | CAST | On demand | Manually |
| AES-GCM - Encrypt (A7376) | KAT | CAST | On demand | Manually |
| AES-GCM - Decrypt (A7145) | KAT | CAST | On demand | Manually |
| AES-GCM - Decrypt (A7151) | KAT | CAST | On demand | Manually |
| AES-GCM - Decrypt (A7152) | KAT | CAST | On demand | Manually |
| AES-GCM - Decrypt (A7153) | KAT | CAST | On demand | Manually |
| AES-GCM - Decrypt (A7154) | KAT | CAST | On demand | Manually |
| AES-GCM - Decrypt (A7155) | KAT | CAST | On demand | Manually |
| AES-GCM - Decrypt (A7156) | KAT | CAST | On demand | Manually |
| AES-GCM - Decrypt (A7157) | KAT | CAST | On demand | Manually |
| AES-GCM - Decrypt (A7158) | KAT | CAST | On demand | Manually |

| Algorithm or Test | Test Method | Test Type | Period | Periodic Method |
|---|---|---|---|---|
| AES-GCM - Decrypt (A7371) | KAT | CAST | On demand | Manually |
| AES-GCM - Decrypt (A7372) | KAT | CAST | On demand | Manually |
| AES-GCM - Decrypt (A7373) | KAT | CAST | On demand | Manually |
| AES-GCM - Decrypt (A7374) | KAT | CAST | On demand | Manually |
| AES-GCM - Decrypt (A7375) | KAT | CAST | On demand | Manually |
| AES-GCM - Decrypt (A7376) | KAT | CAST | On demand | Manually |
| AES-XTS Testing Revision 2.0 - Encrypt (A7145) | KAT | CAST | On demand | Manually |
| AES-XTS Testing Revision 2.0 - Encrypt (A7153) | KAT | CAST | On demand | Manually |
| AES-XTS Testing Revision 2.0 - Encrypt (A7156) | KAT | CAST | On demand | Manually |
| AES-XTS Testing Revision 2.0 - Encrypt (A7371) | KAT | CAST | On demand | Manually |
| AES-XTS Testing Revision 2.0 - Encrypt (A7374) | KAT | CAST | On demand | Manually |
| AES-XTS Testing Revision 2.0 - Encrypt (A7420) | KAT | CAST | On demand | Manually |

| Algorithm or Test | Test Method | Test Type | Period | Periodic Method |
|---|---|---|---|---|
| AES-XTS Testing Revision 2.0 - Decrypt (A7145) | KAT | CAST | On demand | Manually |
| AES-XTS Testing Revision 2.0 - Decrypt (A7153) | KAT | CAST | On demand | Manually |
| AES-XTS Testing Revision 2.0 - Decrypt (A7156) | KAT | CAST | On demand | Manually |
| AES-XTS Testing Revision 2.0 - Decrypt (A7371) | KAT | CAST | On demand | Manually |
| AES-XTS Testing Revision 2.0 - Decrypt (A7374) | KAT | CAST | On demand | Manually |
| AES-XTS Testing Revision 2.0 - Decrypt (A7420) | KAT | CAST | On demand | Manually |
| AES-CMAC (A7145) | KAT | CAST | On demand | Manually |
| AES-CMAC (A7156) | KAT | CAST | On demand | Manually |
| AES-CMAC (A7371) | KAT | CAST | On demand | Manually |
| AES-CMAC (A7374) | KAT | CAST | On demand | Manually |
| HMAC-SHA-1 (A7145) | KAT | CAST | On demand | Manually |
| HMAC-SHA-1 (A7162) | KAT | CAST | On demand | Manually |

| Algorithm or Test | Test Method | Test Type | Period | Periodic Method |
|---|---|---|---|---|
| HMAC-SHA-1 (A7163) | KAT | CAST | On demand | Manually |
| HMAC-SHA-1 (A7164) | KAT | CAST | On demand | Manually |
| HMAC-SHA-1 (A7374) | KAT | CAST | On demand | Manually |
| HMAC-SHA2-224 (A7145) | KAT | CAST | On demand | Manually |
| HMAC-SHA2-224 (A7162) | KAT | CAST | On demand | Manually |
| HMAC-SHA2-224 (A7163) | KAT | CAST | On demand | Manually |
| HMAC-SHA2-224 (A7164) | KAT | CAST | On demand | Manually |
| HMAC-SHA2-224 (A7374) | KAT | CAST | On demand | Manually |
| HMAC-SHA2-256 (A7145) | KAT | CAST | On demand | Manually |
| HMAC-SHA2-256 (A7162) | KAT | CAST | On demand | Manually |
| HMAC-SHA2-256 (A7163) | KAT | CAST | On demand | Manually |
| HMAC-SHA2-256 (A7164) | KAT | CAST | On demand | Manually |
| HMAC-SHA2-256 (A7374) | KAT | CAST | On demand | Manually |
| HMAC-SHA2-384 (A7145) | KAT | CAST | On demand | Manually |

| Algorithm or Test | Test Method | Test Type | Period | Periodic Method |
|---|---|---|---|---|
| HMAC-SHA2-384 (A7162) | KAT | CAST | On demand | Manually |
| HMAC-SHA2-384 (A7163) | KAT | CAST | On demand | Manually |
| HMAC-SHA2-384 (A7164) | KAT | CAST | On demand | Manually |
| HMAC-SHA2-384 (A7374) | KAT | CAST | On demand | Manually |
| HMAC-SHA2-512 (A7145) | KAT | CAST | On demand | Manually |
| HMAC-SHA2-512 (A7162) | KAT | CAST | On demand | Manually |
| HMAC-SHA2-512 (A7163) | KAT | CAST | On demand | Manually |
| HMAC-SHA2-512 (A7164) | KAT | CAST | On demand | Manually |
| HMAC-SHA2-512 (A7374) | KAT | CAST | On demand | Manually |
| HMAC-SHA3-224 (A7147) | KAT | CAST | On demand | Manually |
| HMAC-SHA3-224 (A7379) | KAT | CAST | On demand | Manually |
| HMAC-SHA3-256 (A7147) | KAT | CAST | On demand | Manually |
| HMAC-SHA3-256 (A7379) | KAT | CAST | On demand | Manually |
| HMAC-SHA3-384 (A7147) | KAT | CAST | On demand | Manually |

| Algorithm or Test | Test Method | Test Type | Period | Periodic Method |
|---|---|---|---|---|
| HMAC-SHA3-384 (A7379) | KAT | CAST | On demand | Manually |
| HMAC-SHA3-512 (A7147) | KAT | CAST | On demand | Manually |
| HMAC-SHA3-512 (A7379) | KAT | CAST | On demand | Manually |
| Counter DRBG (A7145) | KAT | CAST | On demand | Manually |
| Counter DRBG (A7151) | KAT | CAST | On demand | Manually |
| Counter DRBG (A7152) | KAT | CAST | On demand | Manually |
| Counter DRBG (A7153) | KAT | CAST | On demand | Manually |
| Counter DRBG (A7154) | KAT | CAST | On demand | Manually |
| Counter DRBG (A7155) | KAT | CAST | On demand | Manually |
| Counter DRBG (A7156) | KAT | CAST | On demand | Manually |
| Counter DRBG (A7157) | KAT | CAST | On demand | Manually |
| Counter DRBG (A7158) | KAT | CAST | On demand | Manually |
| Counter DRBG (A7371) | KAT | CAST | On demand | Manually |
| Counter DRBG (A7372) | KAT | CAST | On demand | Manually |

| Algorithm or Test | Test Method | Test Type | Period | Periodic Method |
|---|---|---|---|---|
| Counter DRBG (A7373) | KAT | CAST | On demand | Manually |
| Counter DRBG (A7374) | KAT | CAST | On demand | Manually |
| Counter DRBG (A7375) | KAT | CAST | On demand | Manually |
| Counter DRBG (A7376) | KAT | CAST | On demand | Manually |
| Hash DRBG (A7145) | KAT | CAST | On demand | Manually |
| Hash DRBG (A7162) | KAT | CAST | On demand | Manually |
| Hash DRBG (A7163) | KAT | CAST | On demand | Manually |
| Hash DRBG (A7164) | KAT | CAST | On demand | Manually |
| Hash DRBG (A7374) | KAT | CAST | On demand | Manually |
| HMAC DRBG (A7145) | KAT | CAST | On demand | Manually |
| HMAC DRBG (A7162) | KAT | CAST | On demand | Manually |
| HMAC DRBG (A7163) | KAT | CAST | On demand | Manually |
| HMAC DRBG (A7164) | KAT | CAST | On demand | Manually |
| HMAC DRBG (A7374) | KAT | CAST | On demand | Manually |

| Algorithm or Test | Test Method | Test Type | Period | Periodic Method |
|---|---|---|---|---|
| ECDSA SigVer (FIPS186-5) (A7146) | KAT | CAST | On demand | Manually |
| RSA SigVer (FIPS186-5) (A7145) | KAT | CAST | On demand | Manually |
| RSA SigVer (FIPS186-5) (A7162) | KAT | CAST | On demand | Manually |
| RSA SigVer (FIPS186-5) (A7163) | KAT | CAST | On demand | Manually |
| RSA SigVer (FIPS186-5) (A7164) | KAT | CAST | On demand | Manually |
| RSA SigVer (FIPS186-5) (A7374) | KAT | CAST | On demand | Manually |
| KAS-FFC-SSC Sp800-56Ar3 (A7144) | KAT | CAST | On demand | Manually |
| Safe Primes Key Generation (A7144) | PCT | PCT | On demand | Manually |
| Entropy Source - Init RCT | RCT | CAST | On demand | Manually |
| Entropy Source - Init APT | APT | CAST | On demand | Manually |
| Entropy Source - Continuous RCT | RCT | CAST | N/A | N/A |

| Algorithm or Test | Test Method | Test Type | Period | Periodic Method |
|---|---|---|---|---|
| Entropy Source - Continuous APT | APT | CAST | N/A | N/A |

Table 24: Conditional Periodic Information

## 10.4 Error States

| Name | Description | Conditions | Recovery Method | Indicator |
|---|---|---|---|---|
| Error State | The Linux kernel immediately stops executing | Any self-test failure | Restart of the module | Kernel Panic |

Table 25: Error States

In the Error State, the output interface is inhibited, and the module accepts no more inputs or requests (as the module is no longer running).

## 10.5 Operator Initiation of Self-Tests

All self-tests, with the exception of the continuous health tests, can be invoked on demand by unloading and subsequently re-initializing the module.

# 11 Life-Cycle Assurance

## 11.1 Installation, Initialization, and Startup Procedures

The module is distributed as a part of the Red Hat Enterprise Linux 9 (RHEL 9) package in the form of the kernel-5.14.0-427.124.1.el9_4, libkcapi-1.4.0-2.el9, and libkcapi-hmaccalc-1.4.0-2.el9 RPM packages.

The module can achieve the approved mode by:

- For installation add the fips=1 option to the kernel command line during the system installation. During the software selection stage, do not install any third-party software. More information can be found at the vendor documentation.
- Switching the system into the approved mode the installation. Execute the fips-mode-setup --enable command. Restart the system. More information can be found at the vendor documentation.

In both cases, the Crypto Officer must verify the RHEL 9 system operates in the approved mode by executing the "fips-mode-setup --check" command, which should output "FIPS mode is enabled."

## 11.2 Administrator Guidance

After installation of the kernel-5.14.0-427.124.1.el9_4, libkcapi-1.4.0-2.el9, and libkcapi-hmaccalc-1.4.0-2.el9 RPM packages, the Crypto Officer must execute the "cat /proc/sys/crypto/fips_name" command. The Crypto Officer must ensure that the proper name is listed in the output as follows:

*Red Hat Enterprise Linux 9 - Kernel Cryptographic API*

Then, the Crypto Officer must execute the "cat /proc/sys/crypto/fips_version" and "rpm -q libkcapi" commands. These commands must output the following for each tested operational environment (one line per output):

**Dell PowerEdge R440:**
***$ cat /proc/sys/crypto/fips_version***
*5.14.0-427.124.1.el9_4.x86_64*

***$ rpm -q libkcapi***
*1.4.0-2.el9.x86_64*

**IBM z16 3931-A01:**
***$ cat /proc/sys/crypto/fips_version***
*5.14.0-427.124.1.el9_4.s390x*

***$ rpm -q libkcapi***
*1.4.0-2.el9.s390x*

**IBM 9080-HEX:**
***$ cat /proc/sys/crypto/fips_version***
*5.14.0-427.124.1.el9_4.ppc64le*

***$ rpm -q libkcapi***
*1.4.0-2.el9.ppc64le*

## 11.3 Non-Administrator Guidance

There is no non-administrator guidance.

## 11.4 Design and Rules

Not applicable for this module.

## 11.5 Maintenance Requirements

There are no maintenance requirements.

## 11.6 End of Life

As the module does not persistently store SSPs, secure sanitization of the module consists of unloading the module. This will zeroize all SSPs in volatile memory. Then, if desired, the kernel-5.14.0-427.124.1.el9_4, libkcapi-1.4.0-2.el9, and libkcapi-hmaccalc-1.4.0-2.el9 RPM packages can be uninstalled from the RHEL 9 system.

# 12 Mitigation of Other Attacks

The module does not offer mitigation of other attacks and therefore this section is not applicable.

# Appendix A. Glossary and Abbreviations

| | |
|---|---|
| AES | Advanced Encryption Standard |
| AES-NI | Advanced Encryption Standard New Instructions |
| API | Application Programming Interface |
| CAST | Cryptographic Algorithm Self-Test |
| CAVP | Cryptographic Algorithm Validation Program |
| CBC | Cipher Block Chaining |
| CCM | Counter with Cipher Block Chaining-Message Authentication Code |
| CFB | Cipher Feedback |
| CKG | Cryptographic Key Generation |
| CMAC | Cipher-based Message Authentication Code |
| CMVP | Cryptographic Module Validation Program |
| CSP | Critical Security Parameter |
| CTR | Counter |
| DH | Diffie-Hellman |
| DRBG | Deterministic Random Bit Generator |
| ECB | Electronic Code Book |
| ECDSA | Elliptic Curve Digital Signature Algorithm |
| FFC | Finite Field Cryptography |
| FIPS | Federal Information Processing Standards |
| GCM | Galois Counter Mode |
| GMAC | Galois Counter Mode Message Authentication Code |

| | |
|---|---|
| HMAC | Keyed-Hash Message Authentication Code |
| IPsec | Internet Protocol Security |
| KAS | Key Agreement Scheme |
| KAT | Known Answer Test |
| MAC | Message Authentication Code |
| NIST | National Institute of Science and Technology |
| OFB | Output Feedback |
| PAA | Processor Algorithm Acceleration |
| PAI | Processor Algorithm Implementation |
| PCT | Pair-wise Consistency Test |
| PKCS | Public-Key Cryptography Standards |
| RSA | Rivest, Shamir, Addleman |
| SHA | Secure Hash Algorithm |
| SSC | Shared Secret Computation |
| SSP | Sensitive Security Parameter |
| XTS | XEX-based Tweaked-codebook mode with cipher text Stealing |

# Appendix B. References


| | |
|---|---|
| FIPS 140-3 | **FIPS PUB 140-3 - Security Requirements For Cryptographic Modules**<br>March 2019<br>https://doi.org/10.6028/NIST.FIPS.140-3 |
| FIPS 140-3 IG | **Implementation Guidance for FIPS PUB 140-3 and the Cryptographic Module Validation Program**<br>18 April 2025<br>https://csrc.nist.gov/Projects/cryptographic-module-validation-program/fips-140-3-ig-announcements |
| FIPS 180-4 | **Secure Hash Standard (SHS)**<br>March 2012<br>https://doi.org/10.6028/NIST.FIPS.180-4 |
| FIPS 186-5 | **Digital Signature Standard (DSS)**<br>February 2023<br>https://doi.org/10.6028/NIST.FIPS.186-5 |
| FIPS 197 | **Advanced Encryption Standard**<br>May 2023<br>https://doi.org/10.6028/NIST.FIPS.197-upd1 |
| FIPS 198-1 | **The Keyed Hash Message Authentication Code (HMAC)**<br>July 2008<br>https://doi.org/10.6028/NIST.FIPS.198-1 |
| FIPS 202 | **SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions**<br>August 2015<br>https://doi.org/10.6028/NIST.FIPS.202 |
| PKCS#1 | **Public Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1**<br>February 2003<br>https://www.ietf.org/rfc/rfc3447.txt |

| | |
|---|---|
| RFC 4106 | **The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)**<br>June 2005<br>https://www.rfc-editor.org/rfc/rfc4106.txt |
| RFC 7296 | **Internet Key Exchange Protocol Version 2 (IKEv2)**<br>June 2005<br>https://www.rfc-editor.org/rfc/rfc7296.txt |
| SP 800-38A | **Recommendation for Block Cipher Modes of Operation Methods and Techniques**<br>December 2001<br>https://doi.org/10.6028/NIST.SP.800-38A |
| SP 800-38B | **Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication**<br>May 2005<br>https://doi.org/10.6028/NIST.SP.800-38B |
| SP 800-38C | **Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality**<br>May 2004<br>https://doi.org/10.6028/NIST.SP.800-38C |
| SP 800-38D | **Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC**<br>November 2007<br>https://doi.org/10.6028/NIST.SP.800-38D |
| SP 800-38E | **Recommendation for Block Cipher Modes of Operation: The XTS AES Mode for Confidentiality on Storage Devices**<br>January 2010<br>https://doi.org/10.6028/NIST.SP.800-38E |
| SP 800-56A Rev. 3 | **Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography**<br>April 2018<br>https://doi.org/10.6028/NIST.SP.800-56Ar3 |

SP 800-90A Rev. 1 **Recommendation for Random Number Generation Using Deterministic Random Bit Generators**
June 2015
https://doi.org/10.6028/NIST.SP.800-90Ar1

SP 800-133 Rev. 2 **Recommendation for Cryptographic Key Generation**
June 2020
https://doi.org/10.6028/NIST.SP.800-133r2