



# Red Hat

Red Hat, Inc.

Red Hat Enterprise Linux 9 Kernel Cryptographic API

FIPS 140-3 Non-Proprietary Security Policy

Document Version: 1.1

Last Modified: 06/23/2025

Prepared by:

atsec information security corporation

4516 Seton Center Pkwy, Suite 250

Austin, TX 78759

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

© 2024 Red Hat, Inc./ atsec information security.  
This document can be reproduced and distributed only whole and intact, including this copyright notice.

# Table of Contents

1 General.....	5
1.1 Overview.....	5
1.1.1 How this Security Policy was prepared .....	5
1.2 Security Levels .....	5
2 Cryptographic Module Specification .....	6
2.1 Description.....	6
2.2 Tested and Vendor Affirmed Module Version and Identification.....	7
2.3 Excluded Components.....	9
2.4 Modes of Operation .....	9
2.5 Algorithms .....	9
2.6 Security Function Implementations.....	19
2.7 Algorithm Specific Information .....	24
2.7.1 AES GCM IV .....	24
2.7.2 AES XTS.....	25
2.7.3 Legacy Use.....	25
2.8 RBG and Entropy .....	25
2.9 Key Generation .....	26
2.10 Key Establishment.....	26
2.11 Industry Protocols.....	26
3 Cryptographic Module Interfaces.....	27
3.1 Ports and Interfaces.....	27
4 Roles, Services, and Authentication .....	28
4.1 Authentication Methods.....	28
4.2 Roles .....	28
4.3 Approved Services.....	28
4.4 Non-Approved Services .....	33
4.5 External Software/Firmware Loaded .....	33
5 Software/Firmware Security .....	34
5.1 Integrity Techniques.....	34
5.2 Initiate on Demand .....	34
6 Operational Environment .....	35
6.1 Operational Environment Type and Requirements.....	35
6.2 Configuration Settings and Restrictions .....	35
6.3 Additional Information .....	35
7 Physical Security .....	36
8 Non-Invasive Security .....	37

9 Sensitive Security Parameters Management .....	38
9.1 Storage Areas .....	38
9.2 SSP Input-Output Methods .....	38
9.3 SSP Zeroization Methods .....	38
9.4 SSPs .....	39
9.5 Transitions .....	41
10 Self-Tests .....	42
10.1 Pre-Operational Self-Tests .....	42
10.2 Conditional Self-Tests .....	42
10.3 Periodic Self-Test Information .....	68
10.4 Error States .....	75
10.5 Operator Initiation of Self-Tests .....	76
11 Life-Cycle Assurance .....	77
11.1 Installation, Initialization, and Startup Procedures .....	77
11.2 Administrator Guidance .....	77
11.3 Non-Administrator Guidance .....	77
11.4 Design and Rules .....	78
11.5 Maintenance Requirements .....	78
11.6 End of Life .....	78
12 Mitigation of Other Attacks .....	79
Appendix A. Glossary and Abbreviations .....	80
Appendix B. References .....	81

## List of Tables

Table 1: Security Levels .....	5
Table 2: Tested Module Identification - Software, Firmware, Hybrid (Executable Code Sets) ..	8
Table 3: Tested Operational Environments - Software, Firmware, Hybrid .....	8
Table 4: Vendor-Affirmed Operational Environments - Software, Firmware, Hybrid .....	8
Table 5: Modes List and Description .....	9
Table 6: Approved Algorithms .....	19
Table 7: Non-Approved, Not Allowed Algorithms .....	19
Table 8: Security Function Implementations .....	24
Table 9: Entropy Certificates .....	25
Table 10: Entropy Sources .....	25
Table 11: Ports and Interfaces .....	27
Table 12: Roles .....	28
Table 13: Approved Services .....	33
Table 14: Non-Approved Services .....	33
Table 15: Storage Areas .....	38
Table 16: SSP Input-Output Methods .....	38
Table 17: SSP Zeroization Methods .....	39
Table 18: SSP Table 1 .....	40
Table 19: SSP Table 2 .....	41
Table 20: Pre-Operational Self-Tests .....	42
Table 21: Conditional Self-Tests .....	68
Table 22: Pre-Operational Periodic Information .....	69
Table 23: Conditional Periodic Information .....	75
Table 24: Error States .....	76

## List of Figures

Figure 1: Block Diagram .....	7
-------------------------------	---

# 1 General

## 1.1 Overview

This document is the non-proprietary FIPS 140-3 Security Policy for version kernel 5.14.0-284.57.1.el9\_2; libkcapi 1.3.1-3.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

The vendor has provided the non-proprietary Security Policy of the cryptographic module, which was further consolidated into this document by atsec information security together with other vendor-supplied documentation. 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
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 (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:** MultiChipStand

#### **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.

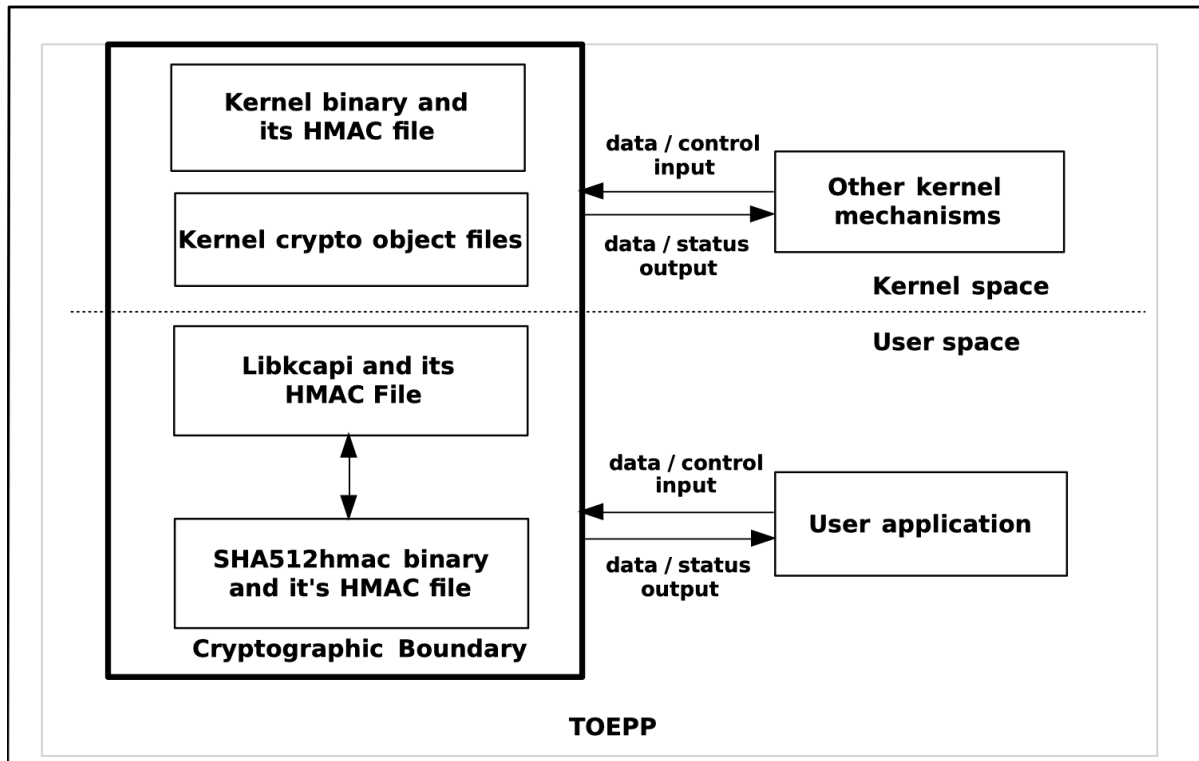


Figure 1: Block Diagram

## 2.2 Tested and Vendor Affirmed Module Version and Identification

### Tested Module Identification - Hardware:

N/A for this module.

### Tested Module Identification - Software, Firmware, Hybrid (Executable Code Sets):

Package or File Name	Software/ Firmware Version	Feature s	Integrity Test
/boot/vmlinuz-5.14.0-284.57.1.el9_2.x86_64 /boot/vmlinuz-5.14.0-284.57.1.el9_2.s390x /boot/vmlinuz-5.14.0-284.57.1.el9_2.ppc64le	5.14.0-284.57.1.el9_2	N/A	HMAC-SHA-512
*.ko and *.ko.xz files in /usr/lib/modules/5.14.0-284.57.1.el9_2.x86_64/kernel/crypto *.ko and *.ko.xz files in /usr/lib/modules/5.14.0-284.57.1.el9_2.x86_64/kernel/arch/x86/crypto *.ko and *.ko.xz files in /usr/lib/modules/5.14.0-284.57.1.el9_2.s390x/kernel/crypto *.ko and *.ko.xz files in /usr/lib/modules/5.14.0-284.57.1.el9_2.s390x/kernel/arch/s390x/crypto *.ko and *.ko.xz files in /usr/lib/modules/5.14.0-284.57.1.el9_2.ppc64le/kernel/crypto	5.14.0-284.57.1.el9_2	N/A	RSA signature verification

Package or File Name	Software/ Firmware Version	Feature s	Integrity Test
*.ko.xz files in /usr/lib/modules/5.14.0-284.57.1.el9_2.ppc64le/kernel/arch/powerpc/crypto			
/usr/lib64/libkcapi.so.1.3.1, /usr/bin/sha512hmac	1.3.1-3.el9	N/A	HMAC SHA-512

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

### Tested Module Identification – Hybrid Disjoint Hardware:

N/A for this module.

### 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(R) Xeon(R) Silver 4216	Yes	N/A	5.14.0-284.57.1.el9_2; 1.3.1-3.el9
Red Hat Enterprise Linux 9	Dell PowerEdge R440	Intel(R) Xeon(R) Silver 4216	No	N/A	5.14.0-284.57.1.el9_2; 1.3.1-3.el9
Red Hat Enterprise Linux 9	IBM z16 3931-A01	IBM z16	Yes	N/A	5.14.0-284.57.1.el9_2; 1.3.1-3.el9
Red Hat Enterprise Linux 9	IBM z16 3931-A01	IBM z16	No	N/A	5.14.0-284.57.1.el9_2; 1.3.1-3.el9
Red Hat Enterprise Linux 9	IBM 9080-HEX	IBM POWER10	Yes	PowerVM FW1040.00 with VIOS 3.1.3.00	5.14.0-284.57.1.el9_2; 1.3.1-3.el9
Red Hat Enterprise Linux 9	IBM 9080-HEX	IBM POWER10	No	PowerVM FW1040.00 with VIOS 3.1.3.00	5.14.0-284.57.1.el9_2; 1.3.1-3.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(R) Xeon(R) 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	Equivalent to the indicator of the requested service as defined in section 4.3
Non-approved mode	Automatically entered whenever a non-approved service is requested.	Non-Approved	Equivalent to the indicator of the requested service as defined in section 4.3

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.

### 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	A5081	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CBC	A5088	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CBC	A5091	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CBC	A5561	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CBC	A5562	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CBC	A5565	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CBC-CS3	A5085	Direction - decrypt, encrypt Key Length - 128, 192, 256	SP 800-38A

Algorithm	CAVP Cert	Properties	Reference
AES-CBC-CS3	A5096	Direction - decrypt, encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CBC-CS3	A5570	Direction - decrypt, encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CCM	A5081	Key Length - 128, 192, 256	SP 800-38C
AES-CCM	A5091	Key Length - 128, 192, 256	SP 800-38C
AES-CCM	A5562	Key Length - 128, 192, 256	SP 800-38C
AES-CCM	A5565	Key Length - 128, 192, 256	SP 800-38C
AES-CFB128	A5083	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CFB128	A5094	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CFB128	A5568	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CMAC	A5081	Direction - Generation, Verification Key Length - 128, 192, 256	SP 800-38B
AES-CMAC	A5091	Direction - Generation, Verification Key Length - 128, 192, 256	SP 800-38B
AES-CMAC	A5562	Direction - Generation, Verification Key Length - 128, 192, 256	SP 800-38B
AES-CMAC	A5565	Direction - Generation, Verification Key Length - 128, 192, 256	SP 800-38B
AES-CTR	A5081	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CTR	A5088	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CTR	A5091	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CTR	A5561	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CTR	A5562	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CTR	A5565	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-ECB	A5081	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-ECB	A5086	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-ECB	A5087	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-ECB	A5088	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-ECB	A5089	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-ECB	A5090	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-ECB	A5091	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-ECB	A5092	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A

Algorithm	CAVP Cert	Properties	Reference
AES-ECB	A5093	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-ECB	A5562	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-ECB	A5563	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-ECB	A5564	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-ECB	A5565	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-ECB	A5566	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-ECB	A5567	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-GCM	A5081	Direction - Decrypt, Encrypt IV Generation - External IV Generation Mode - 8.2.1 Key Length - 128, 192, 256	SP 800-38D
AES-GCM	A5086	Direction - Encrypt IV Generation - Internal IV Generation Mode - 8.2.1 Key Length - 128, 192, 256	SP 800-38D
AES-GCM	A5087	Direction - Decrypt, Encrypt IV Generation - External IV Generation Mode - 8.2.1 Key Length - 128, 192, 256	SP 800-38D
AES-GCM	A5088	Direction - Decrypt, Encrypt IV Generation - External IV Generation Mode - 8.2.1 Key Length - 128, 192, 256	SP 800-38D
AES-GCM	A5089	Direction - Encrypt IV Generation - Internal IV Generation Mode - 8.2.1 Key Length - 128, 192, 256	SP 800-38D
AES-GCM	A5090	Direction - Decrypt, Encrypt IV Generation - External IV Generation Mode - 8.2.1 Key Length - 128, 192, 256	SP 800-38D
AES-GCM	A5091	Direction - Decrypt, Encrypt IV Generation - External IV Generation Mode - 8.2.1 Key Length - 128, 192, 256	SP 800-38D
AES-GCM	A5092	Direction - Encrypt IV Generation - Internal IV Generation Mode - 8.2.1 Key Length - 128, 192, 256	SP 800-38D
AES-GCM	A5093	Direction - Decrypt, Encrypt IV Generation - External IV Generation Mode - 8.2.1 Key Length - 128, 192, 256	SP 800-38D

Algorithm	CAVP Cert	Properties	Reference
AES-GCM	A5562	Direction - Decrypt, Encrypt IV Generation - External Key Length - 128, 192, 256	SP 800-38D
AES-GCM	A5563	Direction - Encrypt IV Generation - Internal IV Generation Mode - 8.2.1 Key Length - 128, 192, 256	SP 800-38D
AES-GCM	A5564	Direction - Decrypt, Encrypt IV Generation - External Key Length - 128, 192, 256	SP 800-38D
AES-GCM	A5565	Direction - Decrypt, Encrypt IV Generation - External Key Length - 128, 192, 256	SP 800-38D
AES-GCM	A5566	Direction - Encrypt IV Generation - Internal IV Generation Mode - 8.2.1 Key Length - 128, 192, 256	SP 800-38D
AES-GCM	A5567	Direction - Decrypt, Encrypt IV Generation - External Key Length - 128, 192, 256	SP 800-38D
AES-GMAC	A5081	Direction - Decrypt, Encrypt IV Generation - External IV Generation Mode - 8.2.1 Key Length - 128, 192, 256	SP 800-38D
AES-GMAC	A5091	Direction - Decrypt, Encrypt IV Generation - External IV Generation Mode - 8.2.1 Key Length - 128, 192, 256	SP 800-38D
AES-GMAC	A5562	Direction - Decrypt, Encrypt IV Generation - External Key Length - 128, 192, 256	SP 800-38D
AES-GMAC	A5565	Direction - Decrypt, Encrypt IV Generation - External Key Length - 128, 192, 256	SP 800-38D
AES-OFB	A5084	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-OFB	A5095	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-OFB	A5569	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-XTS Testing Revision 2.0	A5081	Direction - Decrypt, Encrypt Key Length - 128, 256	SP 800-38E
AES-XTS Testing Revision 2.0	A5088	Direction - Decrypt, Encrypt Key Length - 128, 256	SP 800-38E
AES-XTS Testing Revision 2.0	A5091	Direction - Decrypt, Encrypt Key Length - 128, 256	SP 800-38E
AES-XTS Testing Revision 2.0	A5561	Direction - Decrypt, Encrypt Key Length - 128, 256	SP 800-38E
AES-XTS Testing Revision 2.0	A5562	Direction - Decrypt, Encrypt Key Length - 128, 256	SP 800-38E

Algorithm	CAVP Cert	Properties	Reference
AES-XTS Testing Revision 2.0	A5565	Direction - Decrypt, Encrypt Key Length - 128, 256	SP 800-38E
Counter DRBG	A5081	Prediction Resistance - No, Yes Mode - AES-128, AES-192, AES-256 Derivation Function Enabled - Yes	SP 800-90A Rev. 1
Counter DRBG	A5086	Prediction Resistance - No, Yes Mode - AES-128, AES-192, AES-256 Derivation Function Enabled - Yes	SP 800-90A Rev. 1
Counter DRBG	A5087	Prediction Resistance - No, Yes Mode - AES-128, AES-192, AES-256 Derivation Function Enabled - Yes	SP 800-90A Rev. 1
Counter DRBG	A5088	Prediction Resistance - No, Yes Mode - AES-128, AES-192, AES-256 Derivation Function Enabled - Yes	SP 800-90A Rev. 1
Counter DRBG	A5089	Prediction Resistance - No, Yes Mode - AES-128, AES-192, AES-256 Derivation Function Enabled - Yes	SP 800-90A Rev. 1
Counter DRBG	A5090	Prediction Resistance - No, Yes Mode - AES-128, AES-192, AES-256 Derivation Function Enabled - Yes	SP 800-90A Rev. 1
Counter DRBG	A5091	Prediction Resistance - No, Yes Mode - AES-128, AES-192, AES-256 Derivation Function Enabled - Yes	SP 800-90A Rev. 1
Counter DRBG	A5092	Prediction Resistance - No, Yes Mode - AES-128, AES-192, AES-256 Derivation Function Enabled - Yes	SP 800-90A Rev. 1
Counter DRBG	A5093	Prediction Resistance - No, Yes Mode - AES-128, AES-192, AES-256 Derivation Function Enabled - Yes	SP 800-90A Rev. 1
Counter DRBG	A5562	Prediction Resistance - No, Yes Mode - AES-128, AES-192, AES-256 Derivation Function Enabled - Yes	SP 800-90A Rev. 1
Counter DRBG	A5563	Prediction Resistance - No, Yes Mode - AES-128, AES-192, AES-256 Derivation Function Enabled - Yes	SP 800-90A Rev. 1
Counter DRBG	A5564	Prediction Resistance - No, Yes Mode - AES-128, AES-192, AES-256 Derivation Function Enabled - Yes	SP 800-90A Rev. 1
Counter DRBG	A5565	Prediction Resistance - No, Yes Mode - AES-128, AES-192, AES-256 Derivation Function Enabled - Yes	SP 800-90A Rev. 1
Counter DRBG	A5566	Prediction Resistance - No, Yes Mode - AES-128, AES-192, AES-256 Derivation Function Enabled - Yes	SP 800-90A Rev. 1
Counter DRBG	A5567	Prediction Resistance - No, Yes Mode - AES-128, AES-192, AES-256 Derivation Function Enabled - Yes	SP 800-90A Rev. 1
Hash DRBG	A5081	Prediction Resistance - No, Yes Mode - SHA-1, SHA2-256, SHA2-512	SP 800-90A Rev. 1

Algorithm	CAVP Cert	Properties	Reference
Hash DRBG	A5086	Prediction Resistance - No, Yes Mode - SHA-1, SHA2-256, SHA2-512	SP 800-90A Rev. 1
Hash DRBG	A5087	Prediction Resistance - No, Yes Mode - SHA-1, SHA2-256, SHA2-512	SP 800-90A Rev. 1
Hash DRBG	A5088	Prediction Resistance - No, Yes Mode - SHA-1, SHA2-256, SHA2-512	SP 800-90A Rev. 1
Hash DRBG	A5089	Prediction Resistance - No, Yes Mode - SHA-1, SHA2-256, SHA2-512	SP 800-90A Rev. 1
Hash DRBG	A5090	Prediction Resistance - No, Yes Mode - SHA-1, SHA2-256, SHA2-512	SP 800-90A Rev. 1
Hash DRBG	A5091	Prediction Resistance - No, Yes Mode - SHA-1, SHA2-256, SHA2-512	SP 800-90A Rev. 1
Hash DRBG	A5092	Prediction Resistance - No, Yes Mode - SHA-1, SHA2-256, SHA2-512	SP 800-90A Rev. 1
Hash DRBG	A5093	Prediction Resistance - No, Yes Mode - SHA-1, SHA2-256, SHA2-512	SP 800-90A Rev. 1
Hash DRBG	A5097	Prediction Resistance - No, Yes Mode - SHA-1, SHA2-256, SHA2-512	SP 800-90A Rev. 1
Hash DRBG	A5098	Prediction Resistance - No, Yes Mode - SHA-1, SHA2-256, SHA2-512	SP 800-90A Rev. 1
Hash DRBG	A5099	Prediction Resistance - No, Yes Mode - SHA-1, SHA2-256, SHA2-512	SP 800-90A Rev. 1
Hash DRBG	A5563	Prediction Resistance - No, Yes Mode - SHA-1, SHA2-256, SHA2-512	SP 800-90A Rev. 1
Hash DRBG	A5564	Prediction Resistance - No, Yes Mode - SHA-1, SHA2-256, SHA2-512	SP 800-90A Rev. 1
Hash DRBG	A5565	Prediction Resistance - No, Yes Mode - SHA-1, SHA2-256, SHA2-512	SP 800-90A Rev. 1
Hash DRBG	A5566	Prediction Resistance - No, Yes Mode - SHA-1, SHA2-256, SHA2-512	SP 800-90A Rev. 1
Hash DRBG	A5567	Prediction Resistance - No, Yes Mode - SHA-1, SHA2-256, SHA2-512	SP 800-90A Rev. 1
HMAC DRBG	A5081	Prediction Resistance - No, Yes Mode - SHA-1, SHA2-256, SHA2-512	SP 800-90A Rev. 1
HMAC DRBG	A5086	Prediction Resistance - No, Yes Mode - SHA-1, SHA2-256, SHA2-512	SP 800-90A Rev. 1
HMAC DRBG	A5087	Prediction Resistance - No, Yes Mode - SHA-1, SHA2-256, SHA2-512	SP 800-90A Rev. 1
HMAC DRBG	A5088	Prediction Resistance - No, Yes Mode - SHA-1, SHA2-256, SHA2-512	SP 800-90A Rev. 1
HMAC DRBG	A5089	Prediction Resistance - No, Yes Mode - SHA-1, SHA2-256, SHA2-512	SP 800-90A Rev. 1
HMAC DRBG	A5090	Prediction Resistance - No, Yes Mode - SHA-1, SHA2-256, SHA2-512	SP 800-90A Rev. 1
HMAC DRBG	A5091	Prediction Resistance - No, Yes Mode - SHA-1, SHA2-256, SHA2-512	SP 800-90A Rev. 1
HMAC DRBG	A5092	Prediction Resistance - No, Yes Mode - SHA-1, SHA2-256, SHA2-512	SP 800-90A Rev. 1
HMAC DRBG	A5093	Prediction Resistance - No, Yes Mode - SHA-1, SHA2-256, SHA2-512	SP 800-90A Rev. 1



Algorithm	CAVP Cert	Properties	Reference
HMAC DRBG	A5097	Prediction Resistance - No, Yes Mode - SHA-1, SHA2-256, SHA2-512	SP 800-90A Rev. 1
HMAC DRBG	A5098	Prediction Resistance - No, Yes Mode - SHA-1, SHA2-256, SHA2-512	SP 800-90A Rev. 1
HMAC DRBG	A5099	Prediction Resistance - No, Yes Mode - SHA-1, SHA2-256, SHA2-512	SP 800-90A Rev. 1
HMAC DRBG	A5563	Prediction Resistance - No, Yes Mode - SHA-1, SHA2-256, SHA2-512	SP 800-90A Rev. 1
HMAC DRBG	A5564	Prediction Resistance - No, Yes Mode - SHA-1, SHA2-256, SHA2-512	SP 800-90A Rev. 1
HMAC DRBG	A5565	Prediction Resistance - No, Yes Mode - SHA-1, SHA2-256, SHA2-512	SP 800-90A Rev. 1
HMAC DRBG	A5566	Prediction Resistance - No, Yes Mode - SHA-1, SHA2-256, SHA2-512	SP 800-90A Rev. 1
HMAC DRBG	A5567	Prediction Resistance - No, Yes Mode - SHA-1, SHA2-256, SHA2-512	SP 800-90A Rev. 1
HMAC-SHA-1	A5081	Key Length - Key Length: 112- 524288 Increment 8	FIPS 198-1
HMAC-SHA-1	A5097	Key Length - Key Length: 112- 524288 Increment 8	FIPS 198-1
HMAC-SHA-1	A5098	Key Length - Key Length: 112- 524288 Increment 8	FIPS 198-1
HMAC-SHA-1	A5099	Key Length - Key Length: 112- 524288 Increment 8	FIPS 198-1
HMAC-SHA-1	A5565	Key Length - Key Length: 112- 524288 Increment 8	FIPS 198-1
HMAC-SHA2-224	A5081	Key Length - Key Length: 112- 524288 Increment 8	FIPS 198-1
HMAC-SHA2-224	A5097	Key Length - Key Length: 112- 524288 Increment 8	FIPS 198-1
HMAC-SHA2-224	A5098	Key Length - Key Length: 112- 524288 Increment 8	FIPS 198-1
HMAC-SHA2-224	A5099	Key Length - Key Length: 112- 524288 Increment 8	FIPS 198-1
HMAC-SHA2-224	A5565	Key Length - Key Length: 112- 524288 Increment 8	FIPS 198-1
HMAC-SHA2-256	A5081	Key Length - Key Length: 112- 524288 Increment 8	FIPS 198-1
HMAC-SHA2-256	A5097	Key Length - Key Length: 112- 524288 Increment 8	FIPS 198-1
HMAC-SHA2-256	A5098	Key Length - Key Length: 112- 524288 Increment 8	FIPS 198-1
HMAC-SHA2-256	A5099	Key Length - Key Length: 112- 524288 Increment 8	FIPS 198-1
HMAC-SHA2-256	A5565	Key Length - Key Length: 112- 524288 Increment 8	FIPS 198-1
HMAC-SHA2-384	A5081	Key Length - Key Length: 112- 524288 Increment 8	FIPS 198-1
HMAC-SHA2-384	A5097	Key Length - Key Length: 112- 524288 Increment 8	FIPS 198-1

Algorithm	CAVP Cert	Properties	Reference
HMAC-SHA2-384	A5098	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-384	A5099	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-384	A5565	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-512	A5081	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-512	A5097	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-512	A5098	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-512	A5099	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-512	A5565	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA3-224	A5082	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA3-224	A5571	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA3-256	A5082	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA3-256	A5571	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA3-384	A5082	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA3-384	A5571	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA3-512	A5082	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA3-512	A5571	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
RSA SigVer (FIPS186-4)	A5081	Signature Type - PKCS 1.5 Modulo - 2048, 3072, 4096	FIPS 186-4
RSA SigVer (FIPS186-4)	A5097	Signature Type - PKCS 1.5 Modulo - 2048, 3072, 4096	FIPS 186-4
RSA SigVer (FIPS186-4)	A5098	Signature Type - PKCS 1.5 Modulo - 2048, 3072, 4096	FIPS 186-4
RSA SigVer (FIPS186-4)	A5099	Signature Type - PKCS 1.5 Modulo - 2048, 3072, 4096	FIPS 186-4
RSA SigVer (FIPS186-4)	A5565	Signature Type - PKCS 1.5 Modulo - 2048, 3072, 4096	FIPS 186-4
RSA SigVer (FIPS186-5)	A5081	Modulo - 2048, 3072, 4096 Signature Type - pkcs1v1.5	FIPS 186-5
RSA SigVer (FIPS186-5)	A5097	Modulo - 2048, 3072, 4096 Signature Type - pkcs1v1.5	FIPS 186-5
RSA SigVer (FIPS186-5)	A5098	Modulo - 2048, 3072, 4096 Signature Type - pkcs1v1.5	FIPS 186-5
RSA SigVer (FIPS186-5)	A5099	Modulo - 2048, 3072, 4096 Signature Type - pkcs1v1.5	FIPS 186-5



Algorithm	CAVP Cert	Properties	Reference
RSA SigVer (FIPS186-5)	A5565	Modulo - 2048, 3072, 4096 Signature Type - pkcs1v1.5	FIPS 186-5
SHA-1	A5081	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2	FIPS 180-4
SHA-1	A5097	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2	FIPS 180-4
SHA-1	A5098	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2	FIPS 180-4
SHA-1	A5099	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2	FIPS 180-4
SHA-1	A5565	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2	FIPS 180-4
SHA2-224	A5081	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2	FIPS 180-4
SHA2-224	A5097	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2	FIPS 180-4
SHA2-224	A5098	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2	FIPS 180-4
SHA2-224	A5099	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2	FIPS 180-4
SHA2-224	A5565	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2	FIPS 180-4
SHA2-256	A5081	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2	FIPS 180-4
SHA2-256	A5097	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2	FIPS 180-4
SHA2-256	A5098	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2	FIPS 180-4
SHA2-256	A5099	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2	FIPS 180-4
SHA2-256	A5565	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2	FIPS 180-4
SHA2-384	A5081	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2	FIPS 180-4

Algorithm	CAVP Cert	Properties	Reference
SHA2-384	A5097	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2	FIPS 180-4
SHA2-384	A5098	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2	FIPS 180-4
SHA2-384	A5099	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2	FIPS 180-4
SHA2-384	A5565	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2	FIPS 180-4
SHA2-512	A5081	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2	FIPS 180-4
SHA2-512	A5097	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2	FIPS 180-4
SHA2-512	A5098	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2	FIPS 180-4
SHA2-512	A5099	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2	FIPS 180-4
SHA2-512	A5565	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2	FIPS 180-4
SHA3-224	A5082	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2	FIPS 202
SHA3-224	A5571	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2	FIPS 202
SHA3-256	A5082	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2	FIPS 202
SHA3-256	A5571	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2	FIPS 202
SHA3-384	A5082	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2	FIPS 202
SHA3-384	A5571	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2	FIPS 202
SHA3-512	A5082	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2	FIPS 202

Algorithm	CAVP Cert	Properties	Reference
SHA3-512	A5571	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2	FIPS 202

Table 6: Approved Algorithms

#### Vendor-Affirmed Algorithms:

N/A for this module.

#### 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
KBKDF (libkcapi)	Key derivation
HKDF (libkcapi)	Key derivation
PBKDF2 (libkcapi)	Password-based key derivation
RSA	Encryption primitive; Decryption primitive
RSA with PKCS#1 v1.5 padding	Signature generation (pre-hashed message); Signature verification (pre-hashed message); Key encapsulation; Key un-encapsulation

Table 7: Non-Approved, Not Allowed Algorithms

## 2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
Encryption with AES	BC-UnAuth	Encrypt a plaintext with AES	Key size(s):128, 192, 256 bits (XTS mode 128 and 256 bits only)	AES-CBC: (A5081, A5088, A5091, A5561, A5562, A5565) AES-CBC-CS3: (A5085, A5096, A5570) AES-CFB128: (A5083, A5094, A5568) AES-CTR: (A5081, A5088, A5091, A5561, A5562, A5565) AES-ECB:

Name	Type	Description	Properties	Algorithms
				(A5081, A5086, A5087, A5088, A5089, A5090, A5091, A5092, A5093, A5562, A5563, A5564, A5565, A5566, A5567) AES-OFB: (A5084, A5095, A5569) AES-XTS Testing Revision 2.0: (A5081, A5088, A5091, A5561, A5562, A5565)
Decryption with AES	BC-UnAuth	Decrypt a ciphertext with AES	Key size(s):128, 192, 256 bits (XTS mode 128 and 256 bits only)	AES-CBC: (A5081, A5088, A5091, A5561, A5562, A5565) AES-CBC-CS3: (A5085, A5096, A5570) AES-CFB128: (A5083, A5094, A5568) AES-CTR: (A5081, A5088, A5091, A5561, A5562, A5565) AES-ECB: (A5081, A5086, A5087, A5088, A5089, A5090, A5091, A5092, A5093, A5562, A5563, A5564, A5565, A5566, A5567) AES-OFB: (A5084, A5095, A5569) AES-XTS Testing Revision 2.0: (A5081, A5088, A5091, A5561, A5562, A5565)
Hashing	SHA	Compute a message digest		SHA-1: (A5081, A5097, A5098, A5099, A5565)

Name	Type	Description	Properties	Algorithms
				SHA2-224: (A5081, A5097, A5098, A5099, A5565) SHA2-256: (A5081, A5097, A5098, A5099, A5565) SHA2-384: (A5081, A5097, A5098, A5099, A5565) SHA2-512: (A5081, A5097, A5098, A5099, A5565) SHA3-224: (A5082, A5571) SHA3-256: (A5082, A5571) SHA3-384: (A5082, A5571) SHA3-512: (A5082, A5571)
Message authentication	MAC	Compute a MAC tag for authentication	HMAC key size(s):112-524288 bits (112-256 bits) AES key size(s):128, 192, 256 bits	AES-CMAC: (A5081, A5091, A5562, A5565) AES-GMAC: (A5081, A5091, A5562, A5565) HMAC-SHA-1: (A5081, A5097, A5098, A5099, A5565) HMAC-SHA2-224: (A5081, A5097, A5098, A5099, A5565) HMAC-SHA2-256: (A5081, A5097, A5098, A5099, A5565) HMAC-SHA2-384: (A5081, A5097, A5098, A5099, A5565) HMAC-SHA2-512: (A5081, A5097, A5098, A5099, A5565) HMAC-SHA3-224: (A5082,

Name	Type	Description	Properties	Algorithms
				A5571) HMAC-SHA3-256: (A5082, A5571) HMAC-SHA3-384: (A5082, A5571) HMAC-SHA3-512: (A5082, A5571)
Random number generation with DRBGs	DRBG	Generate random numbers from DRBGs		Counter DRBG: (A5081, A5086, A5087, A5088, A5089, A5090, A5091, A5092, A5093, A5562, A5563, A5564, A5565, A5566, A5567) Hash DRBG: (A5081, A5086, A5087, A5088, A5089, A5090, A5091, A5092, A5093, A5097, A5098, A5099, A5563, A5564, A5565, A5566, A5567) HMAC DRBG: (A5081, A5086, A5087, A5088, A5089, A5090, A5091, A5092, A5093, A5097, A5098, A5099, A5563, A5564, A5565, A5566, A5567)
Signature verification with RSA	DigSig-SigVer	Verify a signature with RSA	Padding:PKCS#1 v1.5 Hashes:SHA1, SHA-224, SHA-256, SHA-384, SHA-512 Key size(s):2048, 3072, 4096 bits (112, 128, 150 bits)	RSA SigVer (FIPS186-4): (A5081, A5097, A5098, A5099, A5565) RSA SigVer (FIPS186-5): (A5081, A5097, A5098, A5099, A5565)

Name	Type	Description	Properties	Algorithms
Authenticated encryption with AES	BC-Auth	Encrypt and authenticate a plaintext with AES	Key size(s):128, 192, 256 bits	AES-CCM: (A5081, A5091, A5562, A5565) AES-GCM: (A5081, A5086, A5087, A5088, A5089, A5090, A5091, A5092, A5093, A5562, A5563, A5564, A5565, A5566, A5567)
Authenticated decryption with AES	BC-Auth	Decrypt and authenticate a ciphertext with AES	Key size(s):128, 192, 256 bits	AES-CCM: (A5081, A5091, A5562, A5565) AES-GCM: (A5081, A5087, A5088, A5090, A5091, A5092, A5086, A5089, A5093, A5562, A5563, A5564, A5565, A5566, A5567)
AES CCM	KTS-Wrap	Key wrapping; Key unwrapping	Key size(s):128, 192, 256 bits	AES-CCM: (A5081, A5091, A5562, A5565)
AES GCM with internal IV	KTS-Wrap	Key wrapping	Key size(s):128, 192, 256 bits	AES-GCM: (A5086, A5089, A5092, A5563, A5566)
AES GCM with external IV	KTS-Wrap	Key unwrapping	Key sizes(s):128, 192, 256 bits	AES-GCM: (A5081, A5087, A5090, A5091, A5093, A5562, A5564, A5565, A5567, A5088)
AES CBC with HMAC SHA-1, HMAC SHA-256, HMAC SHA-384, or HMAC SHA-512	KTS-Wrap	Key wrapping; Key unwrapping	Key sizes(s):128, 192, 256 bits	AES-CBC: (A5081, A5088, A5091, A5561, A5562, A5565) HMAC-SHA-1: (A5081, A5097, A5098, A5099, A5565) HMAC-SHA2-256: (A5081, A5097, A5098, A5099, A5565) HMAC-SHA2-384: (A5081, A5097, A5098,

Name	Type	Description	Properties	Algorithms
				A5099, A5565) HMAC-SHA2-512: (A5081, A5097, A5098, A5099, A5565)
AES CTR with HMAC SHA-1, HMAC SHA-256, HMAC SHA-384, or HMAC SHA-512	KTS-Wrap	Key wrapping; Key unwrapping	Key size(s):128, 192, 256 bits	AES-CTR: (A5081, A5088, A5091, A5561, A5562, A5565) HMAC-SHA-1: (A5081, A5097, A5098, A5099, A5565) HMAC-SHA2-256: (A5081, A5097, A5098, A5099, A5565) HMAC-SHA2-384: (A5081, A5097, A5098, A5099, A5565) HMAC-SHA2-512: (A5081, A5097, A5098, A5099, A5565)

Table 8: 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.

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 Legacy Use

Digital signature verification using SHA-1 is allowed for legacy use only.

These legacy algorithms can only be used on data that was generated prior to the Legacy Date specified in FIPS 140-3 IG C.M.

## 2.8 RBG and Entropy

Cert Number	Vendor Name
E54	Red Hat, Inc.

Table 9: Entropy Certificates

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
RHEL Kernel CPU Time Jitter RNG Entropy Source	Non-Physical	Red Hat Enterprise Linux 9 on Dell PowerEdge R440 on Intel(R) Xeon(R) Silver 4216; Red Hat Enterprise Linux 9 on IBM z16 3931-A01 on IBM z16; Red Hat Enterprise Linux 9 on PowerVM FW1040.00 with VIOS 3.1.3.00 on IBM 9080 HEX on IBM POWER10	64 bits	59.62 bits	Linear-Feedback Shift Register (LFSR)

Table 10: 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.

The DRBG is initially seeded with 384 output bits from the entropy source (357 bits of entropy) and reseeded with 256 output bits from the entropy source (238 bits of entropy). The module does not offer any service to directly get entropy source output. The entropy source is always internally accessed by the module's DRBG for seeding and reseeding.

## 2.9 Key Generation

The module does not provide key generation.

## 2.10 Key Establishment

As permitted by IG D.G, the module provides key transport methods either by using an approved authenticated encryption mode or by a combination of any approved symmetric encryption mode and an approved authentication method.

Specifically, the module provides the following key transport methods:

- Key wrapping using AES GCM with internal IV with a security strength of 128, 192, or 256 bits.
- Key unwrapping using AES GCM with external IV with a security strength of 128, 192, or 256 bits.
- Key wrapping using AES CCM with a security strength of 128, 192, or 256 bits.
- Key wrapping using AES CBC with HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512 with a security strength of 128, 192, or 256 bits.
- Key wrapping using AES CTR with HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512 with a security strength of 128, 192, or 256 bits

## 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 11: 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.

## 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 12: Roles

The module supports the Crypto Officer role only. This sole role is implicitly and always assumed by the operator of the module. 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	Hashing	Crypto Officer
Key wrapping	Wrap a key	crypto_skcipher_setkey returns 0; crypto_shash_init returns 0	AES key, key to be wrapped	wrapped key	AES CCM AES GCM with internal IV AES GCM with external IV AES CBC with HMAC SHA-1, HMAC SHA-256, HMAC SHA-384, or HMAC SHA-512 AES CTR with HMAC SHA-1, HMAC SHA-256, HMAC	Crypto Officer - AES key: W,E - HMAC key: W,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					SHA-384, or HMAC SHA-512	
Key unwrapping	Unwrap a key	crypto_skcipher_setkey returns 0; crypto_shash_init returns 0	AES key, key to be unwrapped	unwrapped key	AES CCM AES GCM with internal IV AES GCM with external IV AES CBC with HMAC SHA-1, HMAC SHA-256, HMAC SHA-384, or HMAC SHA-512 AES CTR with HMAC SHA-1, HMAC SHA-256, HMAC SHA-384, or HMAC SHA-512	Crypto Officer - AES key: W,E - HMAC key: W,E
Encryption	Encrypt a plaintext	crypto_skcipher_setkey returns 0	AES key, plaintext	Ciphertext	Encryption with AES	Crypto Officer - AES key: W,E
Decryption	Decrypt a ciphertext	crypto_skcipher_setkey returns 0	AES key, ciphertext	Plaintext	Decryption with AES	Crypto Officer - AES key: W,E
Authenticated encryption	Encrypt and authenticate a plaintext	For all except AES GCM: crypto_aead_setkey returns 0; For AES GCM: crypto_aead_get_flags(tfm) has the CRYPTO_TFM_	AES key, plaintext	Ciphertext, MAC tag	Authenticated encryption with AES	Crypto Officer - AES key: W,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
		FIPS_COMPLIANCE flag set				
Authenticated decryption	Encrypt and authenticate a ciphertext	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, MAC tag	Plaintext or failure	Authenticated decryption with AES	Crypto Officer - AES key: W,E
Message authentication	Compute a MAC tag	crypto_shash_init returns 0	AES: AES key, message; HMAC: HMAC key, message	MAC tag	Message authentication	Crypto Officer - AES key: W,E - HMAC key: W,E
Random number generation	Generate random bytes	crypto_rng_get_bytes returns 0	Output length	Random bytes	Random number generation with DRBGs	Crypto Officer - Entropy input: W,E - DRBG seed: G,E - DRBG Internal state (V, Key): G,W,E - DRBG Internal state

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						(V, C): G, W, E
Signature verification	Verify a digital signature	pkcs7_verify returns 0	Message, public key, signature	Pass/fail	Signature verification with RSA	Cryptographer - RSA public key: W, E
Error detection code	Compute an EDC (crc32, crct10dif)	None	Message	EDC	None	Cryptographer
Compression	Compress data (deflate, lz4, lz4hc, lzo, zlibdeflate, zstd)	None	Data	Compressed data	None	Cryptographer
Generic system call	Use the kernel to perform various non-cryptographic operations	None	Identifier, various arguments	Various return values	None	Cryptographer
Show version	Return the module name and version information	None	N/A	Module name and version	None	Cryptographer
Show status	Return the module status	None	N/A	Module status	None	Cryptographer
Self-test	Perform the CASTs and integrity tests	None	N/A	Pass/fail	Encryption with AES Decryption with AES Hashing Message authentication Random	Cryptographer

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					number generation with DRBGs Signature verification with RSA Authenticated encryption with AES Authenticated decryption with AES	
Zeroization	Zeroize all SSPs	None	Any SSP	N/A	None	Cryptographic - AES key: Z - HMAC key: Z - Entropy input: Z - DRBG Internal state (V, Key): Z - DRBG Internal state (V, C): Z - RSA public key: Z



Table 13: 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 external IV encryption	Encrypt 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 or a shared secret	KBKDF (libkcapi) HKDF (libkcapi)	CO
Password-based key derivation	Derive a key from a password	PBKDF2 (libkcapi)	CO
RSA encryption primitive	Compute the raw RSA encryption of a plaintext	RSA	CO
RSA decryption primitive	Compute the raw RSA decryption of a ciphertext	RSA	CO
RSA signature generation (pre-hashed message)	Generate a digital signature for a pre-hashed message	RSA with PKCS#1 v1.5 padding	CO
RSA signature verification (pre-hashed message)	Verify a digital signature for a pre-hashed message	RSA with PKCS#1 v1.5 padding	CO
Key encapsulation	Encapsulate a secret key using RSA with PKCS#1 v1.5 padding	RSA with PKCS#1 v1.5 padding	CO
Key un-encapsulation	Un-encapsulate a secret key using RSA with PKCS#1 v1.5 padding	RSA with PKCS#1 v1.5 padding	CO

Table 14: 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 Linux 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). An HMAC SHA-512 calculation is also performed on the sha512hmac utility and the libkcap library to verify their integrity. The kernel crypto object files listed in section 2.2 are loaded on start-up by the module and verified using RSA signature verification with PKCS#1 v1.5 padding, SHA-256, and a 3072-bit key.

### 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 15: 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	

Table 16: SSP Input-Output Methods

### 9.3 SSP Zeroization Methods

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: <code>crypto_free_skcipher</code> and <code>crypto_free_aead</code> ; HMAC key: <code>crypto_free_shash</code> and <code>crypto_free_ahash</code> ; DRBG internal state: <code>crypto_free_rng</code> ; RSA public key: <code>public_key_free</code>
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	By removing power

Zeroization Method	Description	Rationale	Operator Initiation
		successful removal of power implicitly indicates that the zeroization is complete.	

Table 17: 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 with AES Authenticated decryption with AES AES CCM AES GCM with internal IV AES GCM with external IV AES CBC with HMAC SHA-1, HMAC SHA-256, HMAC SHA-384, or HMAC SHA-512 AES CTR with HMAC SHA-1, HMAC SHA-256, HMAC SHA-384, or HMAC SHA-512
HMAC key	HMAC key	112-256 bits - 112-256 bits	Authentication key - CSP			Message authentication

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
Entropy input	Entropy input used to seed the DRBGs	128-448 bits - 128-256 bits	Entropy input - CSP			Random number generation with DRBGs
DRBG seed	DRBG seed derived from entropy input	CTR_DRBG: 128, 192, 256 bits; Hash_DRBG: 128, 256 bits; HMAC_DRBG: 128, 256 bits - CTR_DRBG: 128, 192, 256 bits; Hash_DRBG: 128, 256 bits; HMAC_DRBG: 128, 256 bits	Seed - CSP	Random number generation with DRBGs		Random number generation with DRBGs
DRBG Internal state (V, Key)	Internal state of CTR_DRBG and HMAC_DRBG instances	CTR_DRBG: 128, 192, 256 bits; HMAC_DRBG: 128, 256 bits - CTR_DRBG: 128, 192, 256 bits; HMAC_DRBG: 128, 256 bits	Internal state - CSP	Random number generation with DRBGs		Random number generation with DRBGs
DRBG Internal state (V, C)	Internal state of Hash_DRBG instances	Hash_DRBG: 128, 256 bits - Hash_DRBG: 128, 256 bits	Internal state - CSP	Random number generation with DRBGs		Random number generation with DRBGs
RSA public key	Public key used for RSA signature verification	2048, 3072, 4096 bits - 112, 128, 150 bits	Public key - PSP			Signature verification with RSA

Table 18: 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	
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		RAM:Plaintext	From generation until DRBG seed/reseed	Free cipher handle Remove power from the module	DRBG seed:Derives
DRBG seed		RAM:Plaintext	While the DRBG is being instantiated	Free cipher handle Remove power from the module	Entropy input:Derived From DRBG Internal state (V, Key):Derives
DRBG Internal state (V, Key)		RAM:Plaintext	From DRBG instantiation until DRBG termination	Free cipher handle Remove power from the module	DRBG seed:Derived From
DRBG Internal state (V, C)		RAM:Plaintext	From DRBG instantiation until DRBG termination	Free cipher handle Remove power from the module	DRBG seed:Derived From
RSA public 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	

Table 19: 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.

The RSA algorithm with SHA-1 as implemented by the module conforms to FIPS 186-4. FIPS 186-4 was withdrawn on February 3, 2024 but FIPS 140-3 IG C.K allows RSA signature verification with SHA-1 under FIPS 186-4 to still be approved.

## 10 Self-Tests

### 10.1 Pre-Operational Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
HMAC-SHA2-512 (A5099)	128-bit key	Message Authentication	SW/FW Integrity	Module becomes operational and services are available for use.	Integrity test for vmlinuz, libkcap and sha512hmac binary
RSA SigVer (FIPS186-5) (A5081)	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 20: 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 (A5081)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA-1 (A5097)	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
SHA-1 (A5098)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA-1 (A5099)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-224 (A5081)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-224 (A5097)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-224 (A5098)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-224 (A5099)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-256 (A5081)	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.		
SHA2-256 (A5097)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-256 (A5098)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-256 (A5099)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-384 (A5081)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-384 (A5097)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-384 (A5098)	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
				available for use.		
SHA2-384 (A5099)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-512 (A5081)	0-8184 bit message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-512 (A5097)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-512 (A5098)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-512 (A5099)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA3-224 (A5082)	0-8184 bit message	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
SHA3-256 (A5082)	0-8184 bit message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA3-384 (A5082)	0-8184 bit message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA3-512 (A5082)	0-8184 bit message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
AES-ECB (A5081)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Encryption, Decryption	Module initialization
AES-ECB (A5086)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Encryption, Decryption	Module initialization
AES-ECB (A5087)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Encryption, Decryption	Module initialization
AES-ECB (A5088)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Encryption, Decryption	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				and services are available for use.		
AES-ECB (A5089)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Encryption, Decryption	Module initialization
AES-ECB (A5090)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Encryption, Decryption	Module initialization
AES-ECB (A5092)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Encryption, Decryption	Module initialization
AES-ECB (A5093)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Encryption, Decryption	Module initialization
AES-ECB (A5091)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Encryption, Decryption	Module initialization
AES-CBC (A5081)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are	Encryption, Decryption	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				available for use.		
AES-CBC (A5088)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Encryption, Decryption	Module initialization
AES-CBC-CS3 (A5096)	128 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Encryption, Decryption	Module initialization
AES-OFB (A5095)	128 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Encryption, Decryption	Module initialization
AES-CFB128 (A5094)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Encryption, Decryption	Module initialization
AES-CTR (A5081)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Encryption, Decryption	Module initialization
AES-CTR (A5091)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Encryption, Decryption	Module initialization



Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-CCM (A5091)	128, 192, 256 bit keys; 128-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Encryption, Decryption	Module initialization
AES-GCM (A5081)	128, 192, 256 bit keys, 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Encryption, Decryption	Module initialization
AES-GCM (A5086)	128, 192, 256 bit keys, 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Encryption	Module initialization
AES-GCM (A5087)	128, 192, 256 bit keys, 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Encryption, Decryption	Module initialization
AES-GCM (A5088)	128, 192, 256 bit keys, 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Encryption, Decryption	Module initialization
AES-GCM (A5089)	128, 192, 256 bit keys, 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Encryption	Module initialization
AES-GCM (A5090)	128, 192, 256 bit keys, 96-bit IVs	KAT	CAST	Module becomes operational	Encryption, Decryption	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				and services are available for use.		
AES-GCM (A5091)	128, 192, 256 bit keys, 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Encryption, Decryption	Module initialization
AES-GCM (A5092)	128, 192, 256 bit keys, 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Encryption	Module initialization
AES-GCM (A5093)	128, 192, 256 bit keys, 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Encryption, Decryption	Module initialization
AES-XTS Testing Revision 2.0 (A5081)	128 and 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Encryption, Decryption	Module initialization
AES-XTS Testing Revision 2.0 (A5091)	128 and 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Encryption, Decryption	Module initialization
AES-CMAC (A5091)	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
				available for use.		
HMAC-SHA-1 (A5081)	32-64 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
HMAC-SHA-1 (A5097)	32-64 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
HMAC-SHA-1 (A5098)	32-64 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
HMAC-SHA-1 (A5099)	32-64 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
HMAC-SHA2-224 (A5081)	32-1048 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
HMAC-SHA2-224 (A5097)	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 (A5098)	32-1048 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
HMAC-SHA2-224 (A5099)	32-1048 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
HMAC-SHA2-256 (A5081)	32-64 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
HMAC-SHA2-256 (A5097)	32-64 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
HMAC-SHA2-256 (A5098)	32-64 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
HMAC-SHA2-256 (A5099)	32-64 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
HMAC-SHA2-384 (A5081)	32-1048 bit keys	KAT	CAST	Module becomes operational	Message authentication	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				and services are available for use.		
HMAC-SHA2-384 (A5097)	32-1048 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
HMAC-SHA2-384 (A5098)	32-1048 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
HMAC-SHA2-384 (A5099)	32-1048 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
HMAC-SHA2-512 (A5081)	32-1048 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
HMAC-SHA2-512 (A5097)	32-1048 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
HMAC-SHA2-512 (A5098)	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
				available for use.		
HMAC-SHA2-512 (A5099)	32-1048 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
HMAC-SHA3-224 (A5082)	32-1048 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
HMAC-SHA3-256 (A5082)	32-1048 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
HMAC-SHA3-384 (A5082)	32-1048 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
HMAC-SHA3-512 (A5082)	32-1048 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
Counter DRBG (A5081)	128, 192, 256 bit keys With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Seed, Generate	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
Counter DRBG (A5086)	128, 192, 256 bit keys With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Seed, Generate	Module initialization
Counter DRBG (A5087)	128, 192, 256 bit keys With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Seed, Generate	Module initialization
Counter DRBG (A5088)	128, 192, 256 bit keys With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Seed, Generate	Module initialization
Counter DRBG (A5089)	128, 192, 256 bit keys With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Seed, Generate	Module initialization
Counter DRBG (A5090)	128, 192, 256 bit keys With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Seed, Generate	Module initialization
Counter DRBG (A5091)	128, 192, 256 bit keys With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Seed, Generate	Module initialization
Counter DRBG (A5092)	128, 192, 256 bit keys With/without	KAT	CAST	Module becomes operational	Seed, Generate	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
	PR; Health test per section 11.3 of SP 800-90Arev1			and services are available for use.		
Counter DRBG (A5093)	128, 192, 256 bit keys With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Seed, Generate	Module initialization
Hash DRBG (A5081)	SHA-256 With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Seed, Generate	Module initialization
Hash DRBG (A5086)	SHA-256 With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Seed, Generate	Module initialization
Hash DRBG (A5087)	SHA-256 With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Seed, Generate	Module initialization
Hash DRBG (A5088)	SHA-256 With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Seed, Generate	Module initialization
Hash DRBG (A5089)	SHA-256 With/without PR; Health test per section 11.3	KAT	CAST	Module becomes operational and services are	Seed, Generate	Module initialization



Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
	of SP 800-90Arev1			available for use.		
Hash DRBG (A5090)	SHA-256 With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Seed, Generate	Module initialization
Hash DRBG (A5091)	SHA-256 With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Seed, Generate	Module initialization
Hash DRBG (A5092)	SHA-256 With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Seed, Generate	Module initialization
Hash DRBG (A5093)	SHA-256 With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Seed, Generate	Module initialization
Hash DRBG (A5097)	SHA-256 With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Seed, Generate	Module initialization
Hash DRBG (A5098)	SHA-256 With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Seed, Generate	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
Hash DRBG (A5099)	SHA-256 With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Seed, Generate	Module initialization
HMAC DRBG (A5081)	SHA-256, SHA512 With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Seed, Generate	Module initialization
HMAC DRBG (A5086)	SHA-256, SHA512 With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Seed, Generate	Module initialization
HMAC DRBG (A5087)	SHA-256, SHA512 With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Seed, Generate	Module initialization
HMAC DRBG (A5088)	SHA-256, SHA512 With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Seed, Generate	Module initialization
HMAC DRBG (A5089)	SHA-256, SHA512 With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Seed, Generate	Module initialization
HMAC DRBG (A5090)	SHA-256, SHA512 With/without	KAT	CAST	Module becomes operational	Seed, Generate	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
	PR; Health test per section 11.3 of SP 800-90Arev1			and services are available for use.		
HMAC DRBG (A5091)	SHA-256, SHA512 With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Seed, Generate	Module initialization
HMAC DRBG (A5092)	SHA-256, SHA512 With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Seed, Generate	Module initialization
HMAC DRBG (A5093)	SHA-256, SHA512 With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Seed, Generate	Module initialization
HMAC DRBG (A5097)	SHA-256, SHA512 With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Seed, Generate	Module initialization
HMAC DRBG (A5098)	SHA-256, SHA512 With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Seed, Generate	Module initialization
HMAC DRBG (A5099)	SHA-256, SHA512 With/without PR; Health test per section 11.3	KAT	CAST	Module becomes operational and services are	Seed, Generate	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
	of SP 800-90Arev1			available for use.		
RSA SigVer (FIPS186-5) (A5081)	4096-bit key with SHA-256	KAT	CAST	Module becomes operational and services are available for use.	Verify	Module initialization
RSA SigVer (FIPS186-5) (A5097)	4096-bit key with SHA-256	KAT	CAST	Module becomes operational and services are available for use.	Verify	Module initialization
RSA SigVer (FIPS186-5) (A5098)	4096-bit key with SHA-256	KAT	CAST	Module becomes operational and services are available for use.	Verify	Module initialization
Entropy source, start-up RCT	1024 samples	RCT	CAST	Module becomes operational and services are available for use.	Entropy source start-up test	Entropy source initialization
Entropy source, start-up APT	1024 samples	APT	CAST	Module becomes operational and services are available for use.	Entropy source start-up test	Entropy source initialization
Entropy source, continuous RCT	Cutoff C = 61	RCT	CAST	Entropy source is operational	Entropy source continuous test	Continuously
Entropy source, continuous APT	Cutoff C = 355	APT	CAST	Entropy source is operational	Entropy source continuous test	Continuously

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
SHA-1 (A5565)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-224 (A5565)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-256 (A5565)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-384 (A5565)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-512 (A5565)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA3-224 (A5571)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA3-256 (A5571)	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.		
SHA3-384 (A5571)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA3-512 (A5571)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
HMAC-SHA-1 (A5565)	32-64 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
HMAC-SHA2-224 (A5565)	32-1048 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
HMAC-SHA2-256 (A5565)	32-64 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
HMAC-SHA2-384 (A5565)	32-1048 bit keys	KAT	CAST	Module becomes operational and services are	Message authentication	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				available for use.		
HMAC-SHA2-512 (A5565)	32-1048 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
HMAC-SHA3-224 (A5571)	32-1048 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
HMAC-SHA3-256 (A5571)	32-1048 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
HMAC-SHA3-384 (A5571)	32-1048 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
HMAC-SHA3-512 (A5571)	32-1048 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
Counter DRBG (A5562)	128, 192, 256 bit keys With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Seed, Generate	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
Counter DRBG (A5563)	128, 192, 256 bit keys With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Seed, Generate	Module initialization
Counter DRBG (A5564)	128, 192, 256 bit keys With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Seed, Generate	Module initialization
Counter DRBG (A5565)	128, 192, 256 bit keys With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Seed, Generate	Module initialization
Counter DRBG (A5566)	128, 192, 256 bit keys With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Seed, Generate	Module initialization
Counter DRBG (A5567)	128, 192, 256 bit keys With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Seed, Generate	Module initialization
Hash DRBG (A5563)	SHA-256 With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Seed, Generate	Module initialization
Hash DRBG (A5564)	SHA-256 With/without PR; Health	KAT	CAST	Module becomes operational	Seed, Generate	Module initialization



Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
	test per section 11.3 of SP 800-90Arev1			and services are available for use.		
Hash DRBG (A5565)	SHA-256 With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Seed, Generate	Module initialization
Hash DRBG (A5566)	SHA-256 With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Seed, Generate	Module initialization
Hash DRBG (A5567)	SHA-256 With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Seed, Generate	Module initialization
HMAC DRBG (A5563)	SHA-256, SHA512 With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Seed, Generate	Module initialization
HMAC DRBG (A5564)	SHA-256, SHA512 With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Seed, Generate	Module initialization
HMAC DRBG (A5565)	SHA-256, SHA512 With/without PR; Health test per section 11.3	KAT	CAST	Module becomes operational and services are	Seed, Generate	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
	of SP 800-90Arev1			available for use.		
HMAC DRBG (A5566)	SHA-256, SHA512 With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Seed, Generate	Module initialization
HMAC DRBG (A5567)	SHA-256, SHA512 With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Seed, Generate	Module initialization
AES-ECB (A5562)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Encryption, Decryption	Module initialization
AES-ECB (A5563)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Encryption, Decryption	Module initialization
AES-ECB (A5564)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Encryption, Decryption	Module initialization
AES-ECB (A5565)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Encryption, Decryption	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-ECB (A5566)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Encryption, Decryption	Module initialization
AES-ECB (A5567)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Encryption, Decryption	Module initialization
AES-CBC (A5561)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Encryption, Decryption	Module initialization
AES-GCM (A5562)	128, 192, 256 bit keys, 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Encryption, Decryption	Module initialization
AES-GCM (A5563)	128, 192, 256 bit keys, 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Encryption, Decryption	Module initialization
AES-GCM (A5564)	128, 192, 256 bit keys, 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Encryption, Decryption	Module initialization
AES-GCM (A5565)	128, 192, 256 bit keys, 96-bit IVs	KAT	CAST	Module becomes operational	Encryption, Decryption	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				and services are available for use.		
AES-GCM (A5566)	128, 192, 256 bit keys, 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Encryption, Decryption	Module initialization
AES-GCM (A5567)	128, 192, 256 bit keys, 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Encryption, Decryption	Module initialization
RSA SigVer (FIPS186-5) (A5099)	4096-bit key with SHA-256	KAT	CAST	Module becomes operational and services are available for use.	Verify	Module initialization
RSA SigVer (FIPS186-5) (A5565)	4096-bit key with SHA-256	KAT	CAST	Module becomes operational and services are available for use.	Verify	Module initialization

Table 21: 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 (A5099)	Message Authentication	SW/FW Integrity	On demand	Manually
RSA SigVer (FIPS186-5) (A5081)	Signature Verification	SW/FW Integrity	On demand	Manually

Table 22: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
SHA-1 (A5081)	KAT	CAST	On demand	Manually
SHA-1 (A5097)	KAT	CAST	On demand	Manually
SHA-1 (A5098)	KAT	CAST	On demand	Manually
SHA-1 (A5099)	KAT	CAST	On demand	Manually
SHA2-224 (A5081)	KAT	CAST	On demand	Manually
SHA2-224 (A5097)	KAT	CAST	On demand	Manually
SHA2-224 (A5098)	KAT	CAST	On demand	Manually
SHA2-224 (A5099)	KAT	CAST	On demand	Manually
SHA2-256 (A5081)	KAT	CAST	On demand	Manually
SHA2-256 (A5097)	KAT	CAST	On demand	Manually
SHA2-256 (A5098)	KAT	CAST	On demand	Manually
SHA2-256 (A5099)	KAT	CAST	On demand	Manually
SHA2-384 (A5081)	KAT	CAST	On demand	Manually
SHA2-384 (A5097)	KAT	CAST	On demand	Manually
SHA2-384 (A5098)	KAT	CAST	On demand	Manually
SHA2-384 (A5099)	KAT	CAST	On demand	Manually
SHA2-512 (A5081)	KAT	CAST	On demand	Manually
SHA2-512 (A5097)	KAT	CAST	On demand	Manually
SHA2-512 (A5098)	KAT	CAST	On demand	Manually
SHA2-512 (A5099)	KAT	CAST	On demand	Manually
SHA3-224 (A5082)	KAT	CAST	On demand	Manually
SHA3-256 (A5082)	KAT	CAST	On demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
SHA3-384 (A5082)	KAT	CAST	On demand	Manually
SHA3-512 (A5082)	KAT	CAST	On demand	Manually
AES-ECB (A5081)	KAT	CAST	On demand	Manually
AES-ECB (A5086)	KAT	CAST	On demand	Manually
AES-ECB (A5087)	KAT	CAST	On demand	Manually
AES-ECB (A5088)	KAT	CAST	On demand	Manually
AES-ECB (A5089)	KAT	CAST	On demand	Manually
AES-ECB (A5090)	KAT	CAST	On demand	Manually
AES-ECB (A5092)	KAT	CAST	On demand	Manually
AES-ECB (A5093)	KAT	CAST	On demand	Manually
AES-ECB (A5091)	KAT	CAST	On demand	Manually
AES-CBC (A5081)	KAT	CAST	On demand	Manually
AES-CBC (A5088)	KAT	CAST	On demand	Manually
AES-CBC-CS3 (A5096)	KAT	CAST	On demand	Manually
AES-OFB (A5095)	KAT	CAST	On demand	Manually
AES-CFB128 (A5094)	KAT	CAST	On demand	Manually
AES-CTR (A5081)	KAT	CAST	On demand	Manually
AES-CTR (A5091)	KAT	CAST	On demand	Manually
AES-CCM (A5091)	KAT	CAST	On demand	Manually
AES-GCM (A5081)	KAT	CAST	On demand	Manually
AES-GCM (A5086)	KAT	CAST	On demand	Manually
AES-GCM (A5087)	KAT	CAST	On demand	Manually
AES-GCM (A5088)	KAT	CAST	On demand	Manually
AES-GCM (A5089)	KAT	CAST	On demand	Manually
AES-GCM (A5090)	KAT	CAST	On demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-GCM (A5091)	KAT	CAST	On demand	Manually
AES-GCM (A5092)	KAT	CAST	On demand	Manually
AES-GCM (A5093)	KAT	CAST	On demand	Manually
AES-XTS Testing Revision 2.0 (A5081)	KAT	CAST	On demand	Manually
AES-XTS Testing Revision 2.0 (A5091)	KAT	CAST	On demand	Manually
AES-CMAC (A5091)	KAT	CAST	On demand	Manually
HMAC-SHA-1 (A5081)	KAT	CAST	On demand	Manually
HMAC-SHA-1 (A5097)	KAT	CAST	On demand	Manually
HMAC-SHA-1 (A5098)	KAT	CAST	On demand	Manually
HMAC-SHA-1 (A5099)	KAT	CAST	On demand	Manually
HMAC-SHA2-224 (A5081)	KAT	CAST	On demand	Manually
HMAC-SHA2-224 (A5097)	KAT	CAST	On demand	Manually
HMAC-SHA2-224 (A5098)	KAT	CAST	On demand	Manually
HMAC-SHA2-224 (A5099)	KAT	CAST	On demand	Manually
HMAC-SHA2-256 (A5081)	KAT	CAST	On demand	Manually
HMAC-SHA2-256 (A5097)	KAT	CAST	On demand	Manually
HMAC-SHA2-256 (A5098)	KAT	CAST	On demand	Manually
HMAC-SHA2-256 (A5099)	KAT	CAST	On demand	Manually
HMAC-SHA2-384 (A5081)	KAT	CAST	On demand	Manually
HMAC-SHA2-384 (A5097)	KAT	CAST	On demand	Manually
HMAC-SHA2-384 (A5098)	KAT	CAST	On demand	Manually
HMAC-SHA2-384 (A5099)	KAT	CAST	On demand	Manually
HMAC-SHA2-512 (A5081)	KAT	CAST	On demand	Manually
HMAC-SHA2-512 (A5097)	KAT	CAST	On demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
HMAC-SHA2-512 (A5098)	KAT	CAST	On demand	Manually
HMAC-SHA2-512 (A5099)	KAT	CAST	On demand	Manually
HMAC-SHA3-224 (A5082)	KAT	CAST	On demand	Manually
HMAC-SHA3-256 (A5082)	KAT	CAST	On demand	Manually
HMAC-SHA3-384 (A5082)	KAT	CAST	On demand	Manually
HMAC-SHA3-512 (A5082)	KAT	CAST	On demand	Manually
Counter DRBG (A5081)	KAT	CAST	On demand	Manually
Counter DRBG (A5086)	KAT	CAST	On demand	Manually
Counter DRBG (A5087)	KAT	CAST	On demand	Manually
Counter DRBG (A5088)	KAT	CAST	On demand	Manually
Counter DRBG (A5089)	KAT	CAST	On demand	Manually
Counter DRBG (A5090)	KAT	CAST	On demand	Manually
Counter DRBG (A5091)	KAT	CAST	On demand	Manually
Counter DRBG (A5092)	KAT	CAST	On demand	Manually
Counter DRBG (A5093)	KAT	CAST	On demand	Manually
Hash DRBG (A5081)	KAT	CAST	On demand	Manually
Hash DRBG (A5086)	KAT	CAST	On demand	Manually
Hash DRBG (A5087)	KAT	CAST	On demand	Manually
Hash DRBG (A5088)	KAT	CAST	On demand	Manually
Hash DRBG (A5089)	KAT	CAST	On demand	Manually
Hash DRBG (A5090)	KAT	CAST	On demand	Manually
Hash DRBG (A5091)	KAT	CAST	On demand	Manually
Hash DRBG (A5092)	KAT	CAST	On demand	Manually
Hash DRBG (A5093)	KAT	CAST	On demand	Manually
Hash DRBG (A5097)	KAT	CAST	On demand	Manually



Algorithm or Test	Test Method	Test Type	Period	Periodic Method
Hash DRBG (A5098)	KAT	CAST	On demand	Manually
Hash DRBG (A5099)	KAT	CAST	On demand	Manually
HMAC DRBG (A5081)	KAT	CAST	On demand	Manually
HMAC DRBG (A5086)	KAT	CAST	On demand	Manually
HMAC DRBG (A5087)	KAT	CAST	On demand	Manually
HMAC DRBG (A5088)	KAT	CAST	On demand	Manually
HMAC DRBG (A5089)	KAT	CAST	On demand	Manually
HMAC DRBG (A5090)	KAT	CAST	On demand	Manually
HMAC DRBG (A5091)	KAT	CAST	On demand	Manually
HMAC DRBG (A5092)	KAT	CAST	On demand	Manually
HMAC DRBG (A5093)	KAT	CAST	On demand	Manually
HMAC DRBG (A5097)	KAT	CAST	On demand	Manually
HMAC DRBG (A5098)	KAT	CAST	On demand	Manually
HMAC DRBG (A5099)	KAT	CAST	On demand	Manually
RSA SigVer (FIPS186-5) (A5081)	KAT	CAST	On demand	Manually
RSA SigVer (FIPS186-5) (A5097)	KAT	CAST	On demand	Manually
RSA SigVer (FIPS186-5) (A5098)	KAT	CAST	On demand	Manually
Entropy source, start-up RCT	RCT	CAST	On demand	Manually
Entropy source, start-up APT	APT	CAST	On demand	Manually
Entropy source, continuous RCT	RCT	CAST	On demand	Manually
Entropy source, continuous APT	APT	CAST	On demand	Manually
SHA-1 (A5565)	KAT	CAST	On demand	Manually
SHA2-224 (A5565)	KAT	CAST	On demand	Manually
SHA2-256 (A5565)	KAT	CAST	On demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
SHA2-384 (A5565)	KAT	CAST	On demand	Manually
SHA2-512 (A5565)	KAT	CAST	On demand	Manually
SHA3-224 (A5571)	KAT	CAST	On demand	Manually
SHA3-256 (A5571)	KAT	CAST	On demand	Manually
SHA3-384 (A5571)	KAT	CAST	On demand	Manually
SHA3-512 (A5571)	KAT	CAST	On demand	Manually
HMAC-SHA-1 (A5565)	KAT	CAST	On demand	Manually
HMAC-SHA2-224 (A5565)	KAT	CAST	On demand	Manually
HMAC-SHA2-256 (A5565)	KAT	CAST	On demand	Manually
HMAC-SHA2-384 (A5565)	KAT	CAST	On demand	Manually
HMAC-SHA2-512 (A5565)	KAT	CAST	On demand	Manually
HMAC-SHA3-224 (A5571)	KAT	CAST	On demand	Manually
HMAC-SHA3-256 (A5571)	KAT	CAST	On demand	Manually
HMAC-SHA3-384 (A5571)	KAT	CAST	On demand	Manually
HMAC-SHA3-512 (A5571)	KAT	CAST	On demand	Manually
Counter DRBG (A5562)	KAT	CAST	On demand	Manually
Counter DRBG (A5563)	KAT	CAST	On demand	Manually
Counter DRBG (A5564)	KAT	CAST	On demand	Manually
Counter DRBG (A5565)	KAT	CAST	On demand	Manually
Counter DRBG (A5566)	KAT	CAST	On demand	Manually
Counter DRBG (A5567)	KAT	CAST	On demand	Manually
Hash DRBG (A5563)	KAT	CAST	On demand	Manually
Hash DRBG (A5564)	KAT	CAST	On demand	Manually
Hash DRBG (A5565)	KAT	CAST	On demand	Manually
Hash DRBG (A5566)	KAT	CAST	On demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
Hash DRBG (A5567)	KAT	CAST	On demand	Manually
HMAC DRBG (A5563)	KAT	CAST	On demand	Manually
HMAC DRBG (A5564)	KAT	CAST	On demand	Manually
HMAC DRBG (A5565)	KAT	CAST	On demand	Manually
HMAC DRBG (A5566)	KAT	CAST	On demand	Manually
HMAC DRBG (A5567)	KAT	CAST	On demand	Manually
AES-ECB (A5562)	KAT	CAST	On demand	Manually
AES-ECB (A5563)	KAT	CAST	On demand	Manually
AES-ECB (A5564)	KAT	CAST	On demand	Manually
AES-ECB (A5565)	KAT	CAST	On demand	Manually
AES-ECB (A5566)	KAT	CAST	On demand	Manually
AES-ECB (A5567)	KAT	CAST	On demand	Manually
AES-CBC (A5561)	KAT	CAST	On demand	Manually
AES-GCM (A5562)	KAT	CAST	On demand	Manually
AES-GCM (A5563)	KAT	CAST	On demand	Manually
AES-GCM (A5564)	KAT	CAST	On demand	Manually
AES-GCM (A5565)	KAT	CAST	On demand	Manually
AES-GCM (A5566)	KAT	CAST	On demand	Manually
AES-GCM (A5567)	KAT	CAST	On demand	Manually
RSA SigVer (FIPS186-5) (A5099)	KAT	CAST	On demand	Manually
RSA SigVer (FIPS186-5) (A5565)	KAT	CAST	On demand	Manually

Table 23: 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 24: 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-5.14.0-284.57.1.el9\_2, libkcapi-1.3.1-3.el9, and libkcapi-hmacalc-1.3.1-3.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-5.14.0-284.57.1.el9\_2, libkcapi-1.3.1-3.el9, and libkcapi-hmacalc-1.3.1-3.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:**

5.14.0-284.57.1.el9\_2.x86\_64  
libkcapi-1.3.1-3.el9.x86\_64

**IBM z16 3931-A01:**

5.14.0-284.57.1.el9\_2.s390x  
libkcapi-1.3.1-3.el9.s390x

**IBM 9080-HEX:**

5.14.0-284.57.1.el9\_2.ppc64le  
libkcapi-1.3.1-3.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-5.14.0-284.57.1.el9_2`, `libkcapi-1.3.1-3.el9`, and `libkcapi-hmacalc-1.3.1-3.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
CMAC	Cipher-based Message Authentication Code
CMVP	Cryptographic Module Validation Program
CSP	Critical Security Parameter
CTR	Counter
DRBG	Deterministic Random Bit Generator
ECB	Electronic Code Book
ENT (NP)	Non-physical Entropy Source
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
KAT	Known Answer Test
MAC	Message Authentication Code
NIST	National Institute of Science and Technology
PAA	Processor Algorithm Acceleration
PKCS	Public-Key Cryptography Standards
RSA	Rivest, Shamir, Addleman
SHA	Secure Hash Algorithm
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**  
March 2019  
<https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-3.pdf>
- FIPS 140-3 IG    **Implementation Guidance for FIPS PUB 140-3 and the Cryptographic Module Validation Program**  
<https://csrc.nist.gov/Projects/cryptographic-module-validation-program/fips-140-3-ig-announcements>
- FIPS 180-4      **Secure Hash Standard (SHS)**  
March 2012  
<https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf>
- FIPS 186-5      **Digital Signature Standard (DSS)**  
February 2023  
<https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-5.pdf>
- FIPS 197        **Advanced Encryption Standard**  
November 2001  
<https://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>
- FIPS 198-1      **The Keyed Hash Message Authentication Code (HMAC)**  
July 2008  
[https://csrc.nist.gov/publications/fips/fips198-1/FIPS-198-1\\_final.pdf](https://csrc.nist.gov/publications/fips/fips198-1/FIPS-198-1_final.pdf)
- FIPS 202        **SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions**  
August 2015  
<https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf>
- PKCS#1        **Public Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1**  
February 2003  
<https://www.ietf.org/rfc/rfc3447.txt>
- RFC 5288        **AES Galois Counter Mode (GCM) Cipher Suites for TLS**  
August 2008  
<https://www.ietf.org/rfc/rfc5288.txt>
- SP 800-38A     **Recommendation for Block Cipher Modes of Operation Methods and Techniques**  
December 2001  
<https://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf>
- SP 800-38A Addendum    **Recommendation for Block Cipher Modes of Operation: Three Variants of Ciphertext Stealing for CBC Mode**  
October 2010  
<https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38a-add.pdf>
- SP 800-38B     **Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication**  
May 2005  
[https://csrc.nist.gov/publications/nistpubs/800-38B/SP\\_800-38B.pdf](https://csrc.nist.gov/publications/nistpubs/800-38B/SP_800-38B.pdf)

SP 800-38C	<b>Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality</b> May 2004 <a href="https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38c.pdf">https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38c.pdf</a>
SP 800-38D	<b>Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC</b> November 2007 <a href="https://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf">https://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf</a>
SP 800-38E	<b>Recommendation for Block Cipher Modes of Operation: The XTS AES Mode for Confidentiality on Storage Devices</b> January 2010 <a href="https://csrc.nist.gov/publications/nistpubs/800-38E/nist-sp-800-38E.pdf">https://csrc.nist.gov/publications/nistpubs/800-38E/nist-sp-800-38E.pdf</a>
SP 800-38F	<b>Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping</b> December 2012 <a href="https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-38F.pdf">https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-38F.pdf</a>
SP 800-90Ar1	<b>Recommendation for Random Number Generation Using Deterministic Random Bit Generators</b> June 2015 <a href="https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90Ar1.pdf">https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90Ar1.pdf</a>
SP 800-90B	<b>Recommendation for the Entropy Sources Used for Random Bit Generation</b> January 2018 <a href="https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90B.pdf">https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90B.pdf</a>
SP 800-131Ar2	<b>Transitioning the Use of Cryptographic Algorithms and Key Lengths</b> March 2019 <a href="https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar2.pdf">https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar2.pdf</a>
SP 800-133r2	<b>Recommendation for Cryptographic Key Generation</b> June 2020 <a href="https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-133r2.pdf">https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-133r2.pdf</a>
SP 800-140B	<b>CMVP Security Policy Requirements</b> March 2020 <a href="https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-140B.pdf">https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-140B.pdf</a>