Cloudlinux Inc., TuxCare division

# Kernel Cryptography Module for AlmaLinux 9

FIPS 140-3 Non-Proprietary Security Policy

Document Version: 1.3

Last Modified: 20/07/2026


Prepared by:
atsec information security corporation
4516 Seton Center Parkway, Suite 250
Austin, TX 78759
www.atsec.com

Prepared for:
Cloudlinux Inc., TuxCare division
2318 Louis Road, Suite B
Palo Alto, CA 94303
www.tuxcare.com

# 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 ..... 8
2.4 Modes of Operation ..... 8
2.5 Algorithms ..... 9
2.6 Security Function Implementations ..... 13
2.7 Algorithm Specific Information ..... 17
2.7.1 AES GCM IV ..... 17
2.7.2 AES XTS ..... 18
2.7.3 RSA ..... 18
2.7.4 Authenticated Encryption / Decryption ..... 18
2.8 RBG and Entropy ..... 18
2.9 Key Generation ..... 19
2.10 Key Establishment ..... 19
2.11 Industry Protocols ..... 19
3 Cryptographic Module Interfaces ..... 20
3.1 Ports and Interfaces ..... 20
4 Roles, Services, and Authentication ..... 21
4.1 Authentication Methods ..... 21
4.2 Roles ..... 21
4.3 Approved Services ..... 21
4.4 Non-Approved Services ..... 25
4.5 External Software/Firmware Loaded ..... 25
5 Software/Firmware Security ..... 26
5.1 Integrity Techniques ..... 26
5.2 Initiate on Demand ..... 26
6 Operational Environment ..... 27

© 2026 Cloudlinux Inc., TuxCare division / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

6.1 Operational Environment Type and Requirements ....27
6.2 Configuration Settings and Restrictions ....27
7 Physical Security ....28
8 Non-Invasive Security ....29
9 Sensitive Security Parameters Management ....30
9.1 Storage Areas ....30
9.2 SSP Input-Output Methods ....30
9.3 SSP Zeroization Methods ....30
9.4 SSPs ....31
9.5 Transitions ....34
10 Self-Tests ....35
10.1 Pre-Operational Self-Tests ....35
10.2 Conditional Self-Tests ....36
10.3 Periodic Self-Test Information ....67
10.4 Error States ....78
10.5 Operator Initiation of Self-Tests ....78
11 Life-Cycle Assurance ....79
11.1 Installation, Initialization, and Startup Procedures ....79
11.2 Administrator Guidance ....79
11.3 Non-Administrator Guidance ....79
11.5 End of Life ....80
12 Mitigation of Other Attacks ....81
Appendix A. Glossary and abbreviations ....82
Appendix B. References ....83

© 2026 Cloudlinux Inc., TuxCare division / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

# List of Tables

Table 1: Security Levels ..... 5
Table 2: Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets) ..... 7
Table 3: Tested Operational Environments - Software, Firmware, Hybrid ..... 8
Table 4: Modes List and Description ..... 9
Table 5: Approved Algorithms ..... 13
Table 6: Non-Approved, Not Allowed Algorithms ..... 13
Table 7: Security Function Implementations ..... 17
Table 8: Entropy Certificates ..... 18
Table 9: Entropy Sources ..... 19
Table 10: Ports and Interfaces ..... 20
Table 11: Roles ..... 21
Table 12: Approved Services ..... 25
Table 13: Non-Approved Services ..... 25
Table 14: Storage Areas ..... 30
Table 15: SSP Input-Output Methods ..... 30
Table 16: SSP Zeroization Methods ..... 31
Table 17: SSP Table 1 ..... 33
Table 18: SSP Table 2 ..... 33
Table 19: Pre-Operational Self-Tests ..... 35
Table 20: Conditional Self-Tests ..... 67
Table 21: Pre-Operational Periodic Information ..... 68
Table 22: Conditional Periodic Information ..... 78
Table 23: Error States ..... 78

# List of Figures

Figure 1: Block Diagram ..... 7

© 2026 Cloudlinux Inc., TuxCare division / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

# 1 General

## 1.1 Overview

This document is the non-proprietary FIPS 140-3 Security Policy for version kernel 5.14.0-284.1101.el9_2.tuxcare.11; libkcapi 1.3.1-3.el9 of the Kernel Cryptography Module for AlmaLinux 9 module. It contains the security rules under which the module must operate and describes how this module meets the requirements as specified in FIPS PUB 140-3 (Federal Information Processing Standards Publication 140-3) for an overall Security Level 1 module.

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

### 1.1.1 How this Security Policy was prepared

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

## 1.2 Security Levels

| Section | Title | Security Level |
|---|---|---|
| 1 | General | 1 |
| 2 | Cryptographic module specification | 1 |
| 3 | Cryptographic module interfaces | 1 |
| 4 | Roles, services, and authentication | 1 |
| 5 | Software/Firmware security | 1 |
| 6 | Operational environment | 1 |
| 7 | Physical security | N/A |
| 8 | Non-invasive security | N/A |
| 9 | Sensitive security parameter management | 1 |
| 10 | Self-tests | 1 |
| 11 | Life-cycle assurance | 1 |
| 12 | Mitigation of other attacks | N/A |
| | Overall Level | 1 |

*Table 1: Security Levels*

© 2026 Cloudlinux Inc., TuxCare division / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

# 2 Cryptographic Module Specification

## 2.1 Description

**Purpose and Use:**

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

**Module Type**: Software

**Module Embodiment**: Multi-Chip Standalone

**Module Characteristics**:

**Cryptographic Boundary:**

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

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

The TOEPP of the module is defined as the general-purpose computer on which the module is installed. The PAA/PAI provided by the processor are located within the module's physical perimeter is outside of the module's cryptographic boundary.

© 2026 Cloudlinux Inc., TuxCare division / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

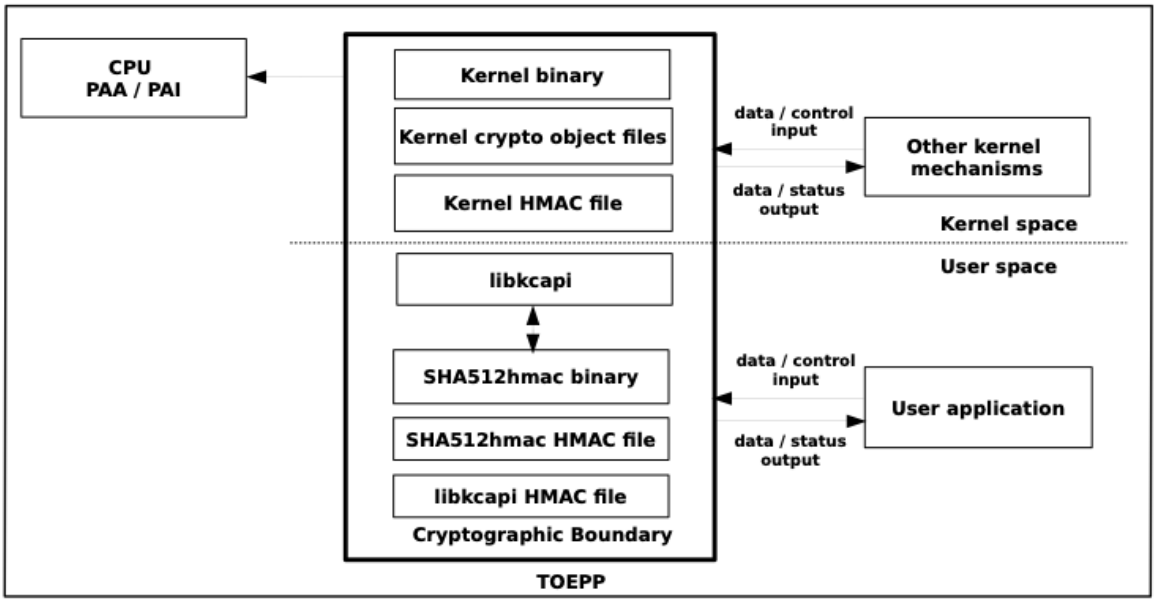


*Figure 1: Block Diagram*

## 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 | Features | Integrity Test |
|---|---|---|---|
| /boot/vmlinuz-5.14.0-284.1101.el9_2.tuxcare.11.x86_64 (for Intel platform), /boot/vmlinuz-5.14.0-284.1101.el9_2.tuxcare.11.aarch64 (for ARM platform) | 5.14.0-284.1101.el9_2.tuxcare.11 | N/A | HMAC-SHA2-512 |
| /usr/lib/modules/5.14.0-284.1101.el9_2.tuxcare.11.x86_64/kernel/crypto/*.ko (for Intel platform), /usr/lib/modules/5.14.0-284.1101.el9_2.tuxcare.11.x86_64/kernel/arch/x86/crypto/*.ko (for Intel platform), /usr/lib/modules/5.14.0-284.1101.el9_2.tuxcare.11.aarch64/kernel/crypto/*.ko (for ARM platform), /usr/lib/modules/5.14.0-284.1101.el9_2.tuxcare.11.aarch64/kernel/arch/arm64/crypto/*.ko (for ARM platform) | 5.14.0-284.1101.el9_2.tuxcare.11 | N/A | Signature Verification with RSA |
| /usr/lib64/libkcapi.so.1.3.1 (for Intel platform), /usr/lib64/libkcapi.so.1.3.1 (for ARM platform), /usr/bin/sha512hmac | 1.3.1-3.el9 | N/A | HMAC-SHA2-512 |

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

© 2026 Cloudlinux Inc., TuxCare division / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

**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) |
|---|---|---|---|---|---|
| AlmaLinux 9.2 | Amazon Web Services (AWS) m5.metal | Intel Xeon Platinum 8259CL | Yes | | kernel 5.14.0-284.1101.el9_2.tuxcare.11; libkcapi 1.3.1-3.el9 |
| AlmaLinux 9.2 | Amazon Web Services (AWS) m5.metal | Intel Xeon Platinum 8259CL | No | | kernel 5.14.0-284.1101.el9_2.tuxcare.11; libkcapi 1.3.1-3.el9 |
| AlmaLinux 9.2 | Amazon Web Services (AWS) a1.metal | AWS Graviton | Yes | | kernel 5.14.0-284.1101.el9_2.tuxcare.11; libkcapi 1.3.1-3.el9 |
| AlmaLinux 9.2 | Amazon Web Services (AWS) a1.metal | AWS Graviton | No | | kernel 5.14.0-284.1101.el9_2.tuxcare.11; libkcapi 1.3.1-3.el9 |

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

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

N/A for this module.

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 |

© 2026 Cloudlinux Inc., TuxCare division / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

| Mode Name | Description | Type | Status Indicator |
|---|---|---|---|
| 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 4: 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 | A4025, A4032, A4033, A4036, A4038, A4041 | Direction - Decrypt, Encrypt<br>Key Length - 128, 192, 256 | SP 800-38A |
| AES-CBC-CS3 | A4029, A4032, A4033, A4046 | Direction - decrypt, encrypt<br>Key Length - 128, 192, 256<br>Payload Length - Payload Length: 128-65536 Increment 8 | SP 800-38A |
| AES-CCM | A4025, A4032, A4033, A4041 | Key Length - 128, 192, 256<br>Tag Length - 112, 128, 32, 48, 64, 80, 96<br>IV Length - IV Length: 56, 64, 72, 80, 88, 96, 104<br>Payload Length - Payload Length: 0-256 Increment 8<br>AAD Length - AAD Length: 0, 256, 65536 | SP 800-38C |
| AES-CFB128 | A4027, A4033, A4044 | Direction - Decrypt, Encrypt<br>Key Length - 128, 192, 256 | SP 800-38A |
| AES-CMAC | A4025, A4032, A4033, A4041 | Direction - Generation, Verification<br>Key Length - 128, 192, 256<br>MAC Length - MAC Length: 128<br>Message Length - Message Length: 8-524288 Increment 8 | SP 800-38B |
| AES-CTR | A4025, A4032, A4033, A4036, A4038, A4041 | Direction - Decrypt, Encrypt<br>Key Length - 128, 192, 256 | SP 800-38A |

© 2026 Cloudlinux Inc., TuxCare division / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

| Algorithm | CAVP Cert | Properties | Reference |
|---|---|---|---|
| | | Payload Length - Payload Length: 8-128 Increment 8<br>Supports Counter larger than maximum value - No<br>Incremental Counter - Yes<br>Counter Tests Performed - Yes | |
| AES-ECB | A4025, A4030, A4031, A4032, A4033, A4034, A4035, A4036, A4038, A4039, A4040, A4041, A4042, A4043 | Direction - Decrypt, Encrypt<br>Key Length - 128, 192, 256 | SP 800-38A |
| AES-GCM | A4025, A4033, A4041 | Direction - Decrypt, Encrypt<br>IV Generation - External<br>IV Generation Mode - 8.2.1<br>Key Length - 128, 192, 256<br>Tag Length - 104, 112, 120, 128, 32, 64, 96<br>IV Length - IV Length: 96<br>Payload Length - Payload Length: 128-65536 Increment 128<br>AAD Length - AAD Length: 128, 256, 120, 0 | SP 800-38D |
| AES-GCM | A4030, A4034, A4039, A4042 | Direction - Encrypt<br>IV Generation - Internal<br>IV Generation Mode - 8.2.1<br>Key Length - 128, 192, 256<br>Tag Length - 128, 64, 96<br>IV Length - IV Length: 96<br>Payload Length - Payload Length: 128, 256, 120, 248<br>AAD Length - AAD Length: 64, 96 | SP 800-38D |
| AES-GCM | A4031, A4035, A4038, A4040, A4043 | Direction - Decrypt, Encrypt<br>IV Generation - External<br>IV Generation Mode - 8.2.1<br>Key Length - 128, 192, 256<br>Tag Length - 128, 64, 96<br>IV Length - IV Length: 96<br>Payload Length - Payload Length: 128, 256, 120, 248<br>AAD Length - AAD Length: 64, 96 | SP 800-38D |
| AES-GMAC | A4025, A4033, A4041 | Direction - Decrypt, Encrypt<br>IV Generation - External<br>IV Generation Mode - 8.2.1<br>Key Length - 128, 192, 256<br>Tag Length - 104, 112, 120, 128, | SP 800-38D |

© 2026 Cloudlinux Inc., TuxCare division / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

| Algorithm | CAVP Cert | Properties | Reference |
|---|---|---|---|
| | | 32, 64, 96<br>IV Length - IV Length: 96<br>AAD Length - AAD Length: 128, 256, 120, 0 | |
| AES-OFB | A4028, A4033, A4045 | Direction - Decrypt, Encrypt<br>Key Length - 128, 192, 256 | SP 800-38A |
| AES-XTS Testing Revision 2.0 | A4025, A4032, A4033, A4036, A4038, A4041 | Direction - Decrypt, Encrypt<br>Key Length - 128, 256<br>Payload Length - Payload Length: 128-65536 Increment 128<br>Tweak Mode - Hex<br>Data Unit Length Matches Payload Length - Yes | SP 800-38E |
| Counter DRBG | A4025, A4030, A4031, A4033, A4034, A4035, A4038, A4039, A4040, A4041, A4042, A4043 | Prediction Resistance - No, Yes<br>Supports Reseed - Yes<br>Mode - AES-128, AES-192, AES-256<br>Derivation Function Enabled - Yes<br>Additional Input - Additional Input: 0<br>Entropy Input - Entropy Input: 128, Entropy Input: 192, Entropy Input: 256<br>Nonce - Nonce: 128, Nonce: 64<br>Personalization String Length - Personalization String Length: 0<br>Returned Bits - 1024, 4096, 512 | SP 800-90A Rev. 1 |
| Hash DRBG | A4025, A4030, A4031, A4034, A4035, A4038, A4039, A4040, A4041, A4042, A4043, A4047, A4048, A4049 | Prediction Resistance - No, Yes<br>Supports Reseed - No<br>Mode - SHA2-256, SHA2-512<br>Entropy Input - Entropy Input: 256<br>Nonce - Nonce: 256<br>Personalization String Length - Personalization String Length: 0<br>Additional Input - Additional Input: 0, 256<br>Returned Bits - 1024, 2048 | SP 800-90A Rev. 1 |
| HMAC DRBG | A4025, A4030, A4031, A4034, A4035, A4038, A4039, A4040, A4041, A4042, A4043, A4047, A4048, A4049 | Prediction Resistance - No, Yes<br>Supports Reseed - No<br>Mode - SHA2-256, SHA2-512<br>Entropy Input - Entropy Input: 256<br>Nonce - Nonce: 256 | SP 800-90A Rev. 1 |

© 2026 Cloudlinux Inc., TuxCare division / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

| Algorithm | CAVP Cert | Properties | Reference |
|---|---|---|---|
| | | Personalization String Length - Personalization String Length: 0<br>Additional Input - Additional Input: 0, 256<br>Returned Bits - 1024, 2048 | |
| HMAC-SHA2-224 | A4025, A4032, A4036, A4037, A4047, A4048, A4049 | MAC - MAC: 224<br>Key Length - Key Length: 112-524288 Increment 8 | FIPS 198-1 |
| HMAC-SHA2-256 | A4025, A4032, A4036, A4037, A4047, A4048, A4049 | MAC - MAC: 256<br>Key Length - Key Length: 112-524288 Increment 8 | FIPS 198-1 |
| HMAC-SHA2-384 | A4025, A4047, A4048, A4049 | MAC - MAC: 384<br>Key Length - Key Length: 112-524288 Increment 8 | FIPS 198-1 |
| HMAC-SHA2-512 | A4025, A4047, A4048, A4049 | MAC - MAC: 512<br>Key Length - Key Length: 112-524288 Increment 8 | FIPS 198-1 |
| HMAC-SHA3-224 | A4026 | MAC - MAC: 224<br>Key Length - Key Length: 112-524288 Increment 8 | FIPS 198-1 |
| HMAC-SHA3-256 | A4026 | MAC - MAC: 256<br>Key Length - Key Length: 112-524288 Increment 8 | FIPS 198-1 |
| HMAC-SHA3-384 | A4026 | MAC - MAC: 384<br>Key Length - Key Length: 112-524288 Increment 8 | FIPS 198-1 |
| HMAC-SHA3-512 | A4026 | MAC - MAC: 512<br>Key Length - Key Length: 112-524288 Increment 8 | FIPS 198-1 |
| RSA SigVer (FIPS186-4) | A4025, A4047, A4048, A4049 | Signature Type - PKCS 1.5<br>Modulo - 2048, 3072, 4096<br>Hash Pair -<br>Hash Algorithm - SHA2-224<br>Public Exponent Mode - Random | FIPS 186-4 |
| SHA2-224 | A4025, A4032, A4036, A4037, A4047, A4048, A4049 | Message Length - Message Length: 0-65536 Increment 8<br>Large Message Sizes - 1, 2 | FIPS 180-4 |
| SHA2-256 | A4025, A4032, A4036, A4037, A4047, A4048, A4049 | Message Length - Message Length: 0-65536 Increment 8<br>Large Message Sizes - 1, 2 | FIPS 180-4 |
| SHA2-384 | A4025, A4047, A4048, A4049 | Message Length - Message Length: 0-65536 Increment 8<br>Large Message Sizes - 1, 2 | FIPS 180-4 |

© 2026 Cloudlinux Inc., TuxCare division / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

| Algorithm | CAVP Cert | Properties | Reference |
|---|---|---|---|
| SHA2-512 | A4025, A4047, A4048, A4049 | Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2 | FIPS 180-4 |
| SHA3-224 | A4026 | Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2 | FIPS 202 |
| SHA3-256 | A4026 | Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2 | FIPS 202 |
| SHA3-384 | A4026 | Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2 | FIPS 202 |
| SHA3-512 | A4026 | Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2 | FIPS 202 |

*Table 5: 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 (pre-hashed message) | Signature generation primitive; Signature verification primitive |

*Table 6: Non-Approved, Not Allowed Algorithms*

## 2.6 Security Function Implementations

© 2026 Cloudlinux Inc., TuxCare division / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

| Name | Type | Description | Properties | Algorithms |
|---|---|---|---|---|
| Symmetric Encryption with AES | BC-UnAuth | Symmetric Encryption using AES | | AES-CBC: (A4025, A4032, A4033, A4036, A4038, A4041)<br>AES-CBC-CS3: (A4029, A4032, A4033, A4046)<br>AES-CFB128: (A4027, A4033, A4044)<br>AES-CTR: (A4025, A4032, A4033, A4036, A4038, A4041)<br>AES-ECB: (A4025, A4030, A4031, A4032, A4033, A4034, A4035, A4036, A4038, A4039, A4040, A4041, A4042, A4043)<br>AES-OFB: (A4028, A4033, A4045)<br>AES-XTS Testing Revision 2.0: (A4025, A4032, A4033, A4036, A4038, A4041) |
| Authenticated Symmetric Encryption with AES | BC-Auth | Encrypt and authenticate a plaintext with AES | | AES-CCM: (A4025, A4032, A4033, A4041)<br>AES-GCM: (A4025, A4030, A4031, A4033, A4034, A4035, A4038, A4039, A4040, A4041, A4042, A4043) |
| Symmetric Decryption with AES | BC-UnAuth | Symmetric Decryption using AES | | AES-CBC: (A4025, A4032, A4033, A4036, A4038, A4041)<br>AES-CBC-CS3: (A4029, A4032, |

© 2026 Cloudlinux Inc., TuxCare division / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

| Name | Type | Description | Properties | Algorithms |
|---|---|---|---|---|
| | | | | A4033, A4046)<br>AES-CFB128: (A4027, A4033, A4044)<br>AES-CTR: (A4025, A4032, A4033, A4036, A4038, A4041)<br>AES-ECB: (A4025, A4030, A4031, A4032, A4033, A4034, A4035, A4036, A4038, A4039, A4040, A4041, A4042, A4043)<br>AES-OFB: (A4028, A4033, A4045)<br>AES-XTS Testing Revision 2.0: (A4025, A4032, A4033, A4036, A4038, A4041) |
| Authenticated Symmetric Decryption with AES | BC-Auth | Decrypt and authenticate a ciphertext with AES | | AES-CCM: (A4025, A4032, A4033, A4041)<br>AES-GCM: (A4025, A4030, A4031, A4033, A4034, A4035, A4038, A4039, A4040, A4041, A4042, A4043) |
| Message Digest with SHA-3 | SHA | Compute a message digest | | SHA3-224: (A4026)<br>SHA3-256: (A4026)<br>SHA3-384: (A4026)<br>SHA3-512: (A4026) |
| Message Digest with SHA-2 | SHA | Compute a message digest | | SHA2-224: (A4025, A4032, A4036, A4037, A4047, A4048, A4049)<br>SHA2-256: (A4025, A4032, A4036, A4037, A4047, A4048, A4049) |

© 2026 Cloudlinux Inc., TuxCare division / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

| Name | Type | Description | Properties | Algorithms |
|---|---|---|---|---|
| | | | | SHA2-384: (A4025, A4047, A4048, A4049)<br>SHA2-512: (A4025, A4047, A4048, A4049) |
| Random Number Generation with CTR_DRBG | DRBG | Generate random bitstrings | | Counter DRBG: (A4025, A4030, A4031, A4033, A4034, A4035, A4038, A4039, A4040, A4041, A4042, A4043) |
| Random Number Generation with HMAC_DRBG | DRBG | Generate random bitstrings | | HMAC DRBG: (A4025, A4030, A4031, A4034, A4035, A4038, A4039, A4040, A4041, A4042, A4043, A4047, A4048, A4049) |
| Random Number Generation with Hash_DRBG | DRBG | Generate random bitstrings | | Hash DRBG: (A4025, A4030, A4031, A4034, A4035, A4038, A4039, A4040, A4041, A4042, A4043, A4047, A4048, A4049) |
| Message Authentication Code (MAC) with HMAC | MAC | Compute a MAC tag | Key length and strength:112-524288 bits (112-256 bits) | HMAC-SHA2-224: (A4025, A4032, A4036, A4037, A4047, A4048, A4049)<br>HMAC-SHA2-256: (A4025, A4032, A4036, A4037, A4047, A4048, A4049)<br>HMAC-SHA2-384: (A4025, A4047, A4048, A4049)<br>HMAC-SHA2-512: (A4025, A4047, A4048, A4049) |

© 2026 Cloudlinux Inc., TuxCare division / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

| Name | Type | Description | Properties | Algorithms |
|---|---|---|---|---|
| | | | | HMAC-SHA3-224: (A4026)<br>HMAC-SHA3-256: (A4026)<br>HMAC-SHA3-384: (A4026)<br>HMAC-SHA3-512: (A4026) |
| Message Authentication Code (MAC) with AES | MAC | Compute a MAC tag | Key length and strength:128, 192, 256 bits | AES-CMAC: (A4025, A4032, A4033, A4041)<br>AES-GMAC: (A4025, A4033, A4041) |
| Signature Verification with RSA | DigSig-SigVer | Internal function for RSA signature verification for integrity test for kernel crypto object files | Mode:PKCS#1 v1.5 with SHA-256<br>Key length and strength:4096 bits with 150 bits of strength | RSA SigVer (FIPS186-4): (A4025, A4047, A4048, A4049) |

*Table 7: 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.

© 2026 Cloudlinux Inc., TuxCare division / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

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.

### 2.7.2 AES XTS

In compliance with FIPS 140-3 IG C.I, the module implements the check to ensure that the two AES keys used in AES XTS algorithm are not identical.

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.

AES-XTS keys (i.e., Key_1 and Key_2) entered into the module shall be generated and/or established independently according to NIST SP 800-133rev2, Section 6.3. for an approved use of AES-XTS.

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

### 2.7.3 RSA

The module provides RSA signature verification as an internal function compliant with IG C.F. The module supports RSA modulus lengths of 4096 bits for signature verification. The RSA signature verification implementation has been tested for all implemented RSA modulus lengths.

### 2.7.4 Authenticated Encryption / Decryption

The module does not establish SSP's using an approved key transport scheme (KTS). However, it does offer approved authenticated algorithms that can be used by an external operator /application as part of an approved KTS.

## 2.8 RBG and Entropy

| Cert Number | Vendor Name |
|---|---|
| E75 | Cloudlinux Inc., TuxCare division |

*Table 8: Entropy Certificates*

| Name | Type | Operational Environment | Sample Size | Entropy per Sample | Conditioning Component |
|---|---|---|---|---|---|
| Cloudlinux Inc., TuxCare division Kernel CPU Time | Non-Physical | AlmaLinux 9.2 running on Amazon Web Services (AWS) m5.metal with Intel Xeon Platinum 8259CL; | 256 bits | Full Entropy | A4026 (SHA3-256) |

© 2026 Cloudlinux Inc., TuxCare division / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

| Name | Type | Operational Environment | Sample Size | Entropy per Sample | Conditioning Component |
|---|---|---|---|---|---|
| Jitter RNG Entropy Source | | AlmaLinux 9.2 running on Amazon Web Services (AWS) a1.metal with AWS Graviton | | | |

*Table 9: Entropy Sources*

## 2.9 Key Generation

The module does not implement any SSP generation methods.

## 2.10 Key Establishment

The module does not implement any SSP establishment methods.

## 2.11 Industry Protocols

AES GCM with internal IV generation in 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.

© 2026 Cloudlinux Inc., TuxCare division / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

# 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 10: Ports and Interfaces*

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

The module does not implement Control Output interface.

© 2026 Cloudlinux Inc., TuxCare division / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

# 4 Roles, Services, and Authentication

## 4.1 Authentication Methods

N/A for this module.

## 4.2 Roles

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

*Table 11: 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 |
|---|---|---|---|---|---|---|
| Symmetric Encryption | Symmetric Encryption using AES | crypto_skcipher_setkey return 0 | Plaintext, AES key | Ciphertext | Symmetric Encryption with AES<br>Authenticated Symmetric Encryption with AES | Crypto Officer<br>- AES key: W,E |
| Symmetric Decryption | Symmetric Decryption using AES | crypto_skcipher_setkey return 0 | Ciphertext, AES key | Plaintext | Symmetric Decryption with AES<br>Authenticated Symmetric Decryption with AES | Crypto Officer<br>- AES key: W,E |
| Authenticated Symmetric 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_FIPS_COMPLIANCE flag set | Plaintext, AES key, IV | Ciphertext, MAC tag | Authenticated Symmetric Encryption with AES | Crypto Officer<br>- AES key: W,E<br>- GCM IV: W,E |

© 2026 Cloudlinux Inc., TuxCare division / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| Authenticated Symmetric Decryption | Decrypt 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 | Ciphertext, AES key, MAC tag, IV | Plaintext | Authenticated Symmetric Decryption with AES | Crypto Officer<br>- AES key: W,E<br>- GCM IV: W,E |
| Message Authentication Code (MAC) | Compute a MAC tag | crypto_shash_init returns 0 | Message, HMAC key | MAC tag | Message Authentication Code (MAC) with AES<br>Message Authentication Code (MAC) with HMAC | Crypto Officer<br>- AES key: W,E<br>- HMAC key: W,E |
| Random Number Generation | Generate random bitstrings | crypto_rng_get_bytes returns 0 | Output length | Random bytes | Random Number Generation with CTR_DRBG<br>Random Number Generation with HMAC_DRBG<br>Random Number Generation with Hash_DRBG | Crypto Officer<br>- Entropy input: W,E<br>- DRBG seed: E,G<br>- DRBG Internal state (V, Key): W,E,G<br>- DRBG Internal state (V, C): W,E,G |
| Message digest | Compute a message digest | crypto_shash_init returns 0 | Message | Digest value | Message Digest with SHA-2<br>Message Digest with SHA-3 | Crypto Officer |
| Compression | Compress data | None | Data | Compressed data | None | Crypto Officer |

© 2026 Cloudlinux Inc., TuxCare division / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| | (deflate, lzo, zlib-deflate) | | | | | |
| Generic system call | Use the kernel to perform various non-cryptographic operations | None | Identifier, various arguments | Various return values | None | Crypto Officer |
| Error detection code | Compute an EDC (crc32, crct10dif) | None | Message | EDC | None | Crypto Officer |
| Show status | Return the module status | None | N/A | Module status | None | Unauthenticated |
| Show module name and version | Return the module name and version information | None | N/A | Module name and version | None | Unauthenticated |
| Self-test | Perform the CASTs and integrity tests | None | N/A | Pass/fail result of self-tests | Signature Verification with RSA Symmetric Encryption with AES Authenticated Symmetric Encryption with AES Symmetric Decryption with AES Authenticated Symmetric Decryption | Unauthenticated |

© 2026 Cloudlinux Inc., TuxCare division / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| | | | | | with AES Message Digest with SHA-3 Message Digest with SHA-2 Random Number Generation with CTR_DRBG Random Number Generation with HMAC_DRBG Random Number Generation with Hash_DRBG Message Authentication Code (MAC) with HMAC Message Authentication Code (MAC) with AES | |
| Zeroization | Zeroize SSPs | None | Any SSP | N/A | None | Crypto Officer<br>- AES key: Z<br>- GCM IV: Z<br>- HMAC key: Z<br>- Entropy input: Z |

© 2026 Cloudlinux Inc., TuxCare division / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| | | | | | | - DRBG seed: Z<br>- DRBG Internal state (V, Key): Z<br>- DRBG Internal state (V, C): Z |

*Table 12: Approved Services*

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

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

## 4.4 Non-Approved Services

| Name | Description | Algorithms | Role |
|---|---|---|---|
| AES GCM with external IV | Encryption | AES GCM with external IV | CO |
| KBKDF (libkcapi) | Key derivation | KBKDF (libkcapi) | CO |
| HKDF (libkcapi) | Key derivation | HKDF (libkcapi) | CO |
| PBKDF2 (libkcapi) | Password-based key derivation | PBKDF2 (libkcapi) | CO |
| RSA | Encryption primitive; Decryption primitive | RSA | CO |
| RSA with PKCS#1 v1.5 padding (pre-hashed message) | Signature generation primitive; Signature verification primitive | RSA with PKCS#1 v1.5 padding (pre-hashed message) | CO |

*Table 13: Non-Approved Services*

## 4.5 External Software/Firmware Loaded

The module does not load external software or firmware.

© 2026 Cloudlinux Inc., TuxCare division / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

# 5 Software/Firmware Security

## 5.1 Integrity Techniques

The Linux kernel binary, libkcapi, and sha512hmac software components are integrity tested using an HMAC-SHA2-512 calculation performed by the sha512hmac utility (which utilizes the module's HMAC and SHA-512 implementations). The kernel crypto object files listed in Table "Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets)" are loaded on start-up by the module and verified using RSA signature verification with PKCS#1 v1.5 padding, SHA-256, and a 4096-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.

© 2026 Cloudlinux Inc., TuxCare division / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

# 6 Operational Environment

## 6.1 Operational Environment Type and Requirements

**Type of Operational Environment**: Modifiable

**How Requirements are Satisfied:**

The approved cryptographic algorithms of the module are part of the Linux kernel, which operates in Linux kernel space. This ensures that any SSPs contained within the module are protected by the process isolation and memory separation mechanisms provided by the Linux kernel, and only the module has control over these SSPs. The user space libkcapi and sha512hmac components, though not processing any SSPs, are similarly protected by the operating environment.

## 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 environment. The use of any of these tools implies that the cryptographic module is running in a non-validated operational environment.

© 2026 Cloudlinux Inc., TuxCare division / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

# 7 Physical Security

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

© 2026 Cloudlinux Inc., TuxCare division / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

# 8 Non-Invasive Security

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

© 2026 Cloudlinux Inc., TuxCare division / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

# 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 14: 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 | Operator calling application (TOEPP) | Cryptographic module | Plaintext | Manual | Electronic | |
| API output parameters | Cryptographic module | Operator calling application (TOEPP) | Plaintext | Manual | Electronic | |

*Table 15: SSP Input-Output Methods*

## 9.3 SSP Zeroization Methods

| Zeroization Method | Description | Rationale | Operator Initiation |
|---|---|---|---|
| Wipe and Free memory block allocated | Zeroizes the SSPs contained within the cipher handle. | Memory occupied by SSPs is overwritten with zeroes and then it is released, which renders the SSP values irretrievable. The completion of the zeroization routine indicates that the zeroization procedure succeeded. | By calling the cipher related zeroization API; AES key: crypto_free_skcipher and crypto_free_aead; HMAC key: crypto_free_shash and crypto_free_ahash; Entropy input, DRBG seed, DRBG Internal state (V, Key), DRBG Internal state (V, C): crypto_free_rng |
| Automatic | Automatically zeroized by the module when no longer needed | Memory occupied by SSPs is overwritten with zeroes, which renders the SSP values irretrievable. | N/A |

© 2026 Cloudlinux Inc., TuxCare division / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

| Zeroization Method | Description | Rationale | Operator Initiation |
|---|---|---|---|
| Module Reset | De-allocates the volatile memory used to store SSPs | Volatile memory used by the module is overwritten within nanoseconds when power is removed. | By unloading and reloading the module |

*Table 16: 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; Authenticated encryption; Authenticated decryption; Message authentication; | XTS: 128, 256 bits; Other modes: 128, 192, 256 bits - XTS: 128, 256 bits; Other modes: 128, 192, 256 bits | Symmetric key - CSP | | | Symmetric Encryption with AES Authenticated Symmetric Encryption with AES Symmetric Decryption with AES Authenticated Symmetric Decryption with AES Message Authentication Code (MAC) with AES |
| HMAC key | HMAC key used for Message authentication; | 112-524288 - 112-256 bits | Symmetric key - CSP | | | Message Authentication Code (MAC) with HMAC |
| Entropy input | Entropy input used for Random number generation; IG D.L compliant | 128-384 bits - 128-384 bits | Entropy Input - CSP | | | Random Number Generation with CTR_DRBG Random Number Generation with |

© 2026 Cloudlinux Inc., TuxCare division / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

| Name | Description | Size - Strength | Type - Category | Generated By | Established By | Used By |
|---|---|---|---|---|---|---|
| | | | | | | HMAC_DRBG Random Number Generation with Hash_DRBG |
| DRBG seed | DRBG seed used for Random number generation; IG D.L compliant | CTR_DRBG: 256, 320, 384 bits; Hash_DRBG: 440 bits, 888 bits; HMAC_DRBG: 440 bits, 888 bits - CTR_DRBG: 128, 192, 256 bits; Hash_DRBG: 128, 256 bits; HMAC_DRBG: 128, 256 bits | Seed - CSP | Random Number Generation with CTR_DRBG Random Number Generation with HMAC_DRBG Random Number Generation with Hash_DRBG | | |
| DRBG Internal state (V, Key) | DRBG Internal state (V, Key) used for Random number generation; IG D.L compliant | CTR_DRBG: 256, 320, 384 bits; HMAC_DRBG: 320, 512, 1024 bits - CTR_DRBG: 128, 192, 256 bits; HMAC_DRBG: 128, 256 bits | Internal state - CSP | Random Number Generation with CTR_DRBG Random Number Generation with HMAC_DRBG | | |
| DRBG Internal state (V, C) | DRBG Internal state (V, C) used for Random number generation; IG D.L compliant | Hash_DRBG: 880, 1776 bits - Hash_DRBG: 128, 256 bits | Internal state - CSP | Random Number Generation with Hash_DRBG | | |
| GCM IV | IV used for Authenticated encryption; | 96 bit - N/A | Initialization vector - PSP | | | Authenticated Symmetric Encryption with AES |

© 2026 Cloudlinux Inc., TuxCare division / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

| Name | Description | Size - Strength | Type - Category | Generated By | Established By | Used By |
|---|---|---|---|---|---|---|
| | Authenticated decryption | | | | | Authenticated Symmetric Decryption with AES |

*Table 17: SSP Table 1*

| Name | Input - Output | Storage | Storage Duration | Zeroization | Related SSPs |
|---|---|---|---|---|---|
| AES key | API input parameters API output parameters | RAM:Plaintext | From service invocation to service completion | Wipe and Free memory block allocated Module Reset | |
| HMAC key | API input parameters API output parameters | RAM:Plaintext | From service invocation to service completion | Wipe and Free memory block allocated Module Reset | |
| Entropy input | API input parameters API output parameters | RAM:Plaintext | From service invocation to service completion | Wipe and Free memory block allocated Module Reset | DRBG seed:Derives |
| DRBG seed | API input parameters API output parameters | RAM:Plaintext | From service invocation to service completion | Wipe and Free memory block allocated Module Reset | Entropy input:Derived From DRBG Internal state (V, Key):Generates DRBG Internal state (V, C):Generates |
| DRBG Internal state (V, Key) | API input parameters API output parameters | RAM:Plaintext | From service invocation to service completion | Wipe and Free memory block allocated Module Reset | DRBG seed:Generated From |
| DRBG Internal state (V, C) | API input parameters API output parameters | RAM:Plaintext | From service invocation to service completion | Wipe and Free memory block allocated Module Reset | DRBG seed:Generated From |
| GCM IV | API output parameters | RAM:Plaintext | From service invocation to service completion | Wipe and Free memory block allocated Module Reset Automatic | |

*Table 18: SSP Table 2*

© 2026 Cloudlinux Inc., TuxCare division / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

## 9.5 Transitions

The RSA algorithm as implemented by the module conforms to FIPS 186-4, which has been superseded by FIPS 186-5. FIPS 186-4 has been withdrawn on February 3, 2024.

© 2026 Cloudlinux Inc., TuxCare division / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

# 10 Self-Tests

## 10.1 Pre-Operational Self-Tests

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details |
|---|---|---|---|---|---|
| HMAC-SHA2-512 (A4025) | 128-bit key | Message Authentication | SW/FW Integrity | Module becomes operational and services are available for use | Integrity test for kernel binary, libkcapi, and sha512hmac software components |
| HMAC-SHA2-512 (A4047) | 128-bit key | Message Authentication | SW/FW Integrity | Module becomes operational and services are available for use | Integrity test for kernel binary, libkcapi, and sha512hmac software components |
| HMAC-SHA2-512 (A4048) | 128-bit key | Message Authentication | SW/FW Integrity | Module becomes operational and services are available for use | Integrity test for kernel binary, libkcapi, and sha512hmac software components |
| HMAC-SHA2-512 (A4049) | 128-bit key | Message Authentication | SW/FW Integrity | Module becomes operational and services are available for use | Integrity test for kernel binary, libkcapi, and sha512hmac software components |
| RSA SigVer (FIPS186-4) (A4025) | 4096-bit key with SHA-256 | Signature Verification | SW/FW Integrity | Module becomes operational and services are available for use | Integrity test for kernel crypto object files |
| RSA SigVer (FIPS186-4) (A4047) | 4096-bit key with SHA-256 | Signature Verification | SW/FW Integrity | Module becomes operational and services are available for use | Integrity test for kernel crypto object files |
| RSA SigVer (FIPS186-4) (A4048) | 4096-bit key with SHA-256 | Signature Verification | SW/FW Integrity | Module becomes operational and services are available for use | Integrity test for kernel crypto object files |
| RSA SigVer (FIPS186-4) (A4049) | 4096-bit key with SHA-256 | Signature Verification | SW/FW Integrity | Module becomes operational and services are available for use | Integrity test for kernel crypto object files |

*Table 19: Pre-Operational Self-Tests*

© 2026 Cloudlinux Inc., TuxCare division / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

The pre-operational software integrity tests are performed automatically when the module is powered on, before the module transitions into the operational state. While the module is executing the self-tests, services are not available, and data output (via the data output interface) is inhibited until the 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 |
|---|---|---|---|---|---|---|
| SHA2-224 (A4025) | 0-8184 bit messages | KAT | CAST | Module becomes operational and services are available for use. | Message digest | Module initialization |
| SHA2-224 (A4032) | 0-8184 bit messages | KAT | CAST | Module becomes operational and services are available for use. | Message digest | Module initialization |
| SHA2-224 (A4036) | 0-8184 bit messages | KAT | CAST | Module becomes operational and services are available for use. | Message digest | Module initialization |
| SHA2-224 (A4037) | 0-8184 bit messages | KAT | CAST | Module becomes operational and services are available for use. | Message digest | Module initialization |
| SHA2-224 (A4047) | 0-8184 bit messages | KAT | CAST | Module becomes operational and services are available for use. | Message digest | Module initialization |
| SHA2-224 (A4048) | 0-8184 bit messages | KAT | CAST | Module becomes operational and services | Message digest | Module initialization |

© 2026 Cloudlinux Inc., TuxCare division / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| | | | | are available for use. | | |
| SHA2-224 (A4049) | 0-8184 bit messages | KAT | CAST | Module becomes operational and services are available for use. | Message digest | Module initialization |
| SHA2-256 (A4025) | 0-8184 bit messages | KAT | CAST | Module becomes operational and services are available for use. | Message digest | Module initialization |
| SHA2-256 (A4032) | 0-8184 bit messages | KAT | CAST | Module becomes operational and services are available for use. | Message digest | Module initialization |
| SHA2-256 (A4036) | 0-8184 bit messages | KAT | CAST | Module becomes operational and services are available for use. | Message digest | Module initialization |
| SHA2-256 (A4037) | 0-8184 bit messages | KAT | CAST | Module becomes operational and services are available for use. | Message digest | Module initialization |
| SHA2-256 (A4047) | 0-8184 bit messages | KAT | CAST | Module becomes operational and services are available for use. | Message digest | Module initialization |
| SHA2-256 (A4048) | 0-8184 bit messages | KAT | CAST | Module becomes operational and services are available for use. | Message digest | Module initialization |

© 2026 Cloudlinux Inc., TuxCare division / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| SHA2-256 (A4049) | 0-8184 bit messages | KAT | CAST | Module becomes operational and services are available for use. | Message digest | Module initialization |
| SHA2-384 (A4025) | 0-8184 bit messages | KAT | CAST | Module becomes operational and services are available for use. | Message digest | Module initialization |
| SHA2-384 (A4047) | 0-8184 bit messages | KAT | CAST | Module becomes operational and services are available for use. | Message digest | Module initialization |
| SHA2-384 (A4048) | 0-8184 bit messages | KAT | CAST | Module becomes operational and services are available for use. | Message digest | Module initialization |
| SHA2-384 (A4049) | 0-8184 bit messages | KAT | CAST | Module becomes operational and services are available for use. | Message digest | Module initialization |
| SHA2-512 (A4025) | 0-8184 bit messages | KAT | CAST | Module becomes operational and services are available for use. | Message digest | Module initialization |
| SHA2-512 (A4047) | 0-8184 bit messages | KAT | CAST | Module becomes operational and services are available for use. | Message digest | Module initialization |
| SHA2-512 (A4048) | 0-8184 bit messages | KAT | CAST | Module becomes | Message digest | Module initialization |

© 2026 Cloudlinux Inc., TuxCare division / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| | | | | operational and services are available for use. | | |
| SHA2-512 (A4049) | 0-8184 bit messages | KAT | CAST | Module becomes operational and services are available for use. | Message digest | Module initialization |
| AES-ECB - Encrypt (A4025) | Encrypt with 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-ECB - Encrypt (A4030) | Encrypt with 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-ECB - Encrypt (A4031) | Encrypt with 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-ECB - Encrypt (A4032) | Encrypt with 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-ECB - Encrypt (A4033) | Encrypt with 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-ECB - Encrypt (A4034) | Encrypt with 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services | Encryption | Module initialization |

© 2026 Cloudlinux Inc., TuxCare division / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| | | | | are available for use. | | |
| AES-ECB - Encrypt (A4035) | Encrypt with 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-ECB - Encrypt (A4036) | Encrypt with 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-ECB - Encrypt (A4038) | Encrypt with 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-ECB - Encrypt (A4039) | Encrypt with 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-ECB - Encrypt (A4040) | Encrypt with 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-ECB - Encrypt (A4041) | Encrypt with 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-ECB - Encrypt (A4042) | Encrypt with 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |

© 2026 Cloudlinux Inc., TuxCare division / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| AES-ECB - Encrypt (A4043) | Encrypt with 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-ECB - Decrypt (A4025) | Decrypt with 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| AES-ECB - Decrypt (A4030) | Decrypt with 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| AES-ECB - Decrypt (A4031) | Decrypt with 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| AES-ECB - Decrypt (A4032) | Decrypt with 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| AES-ECB - Decrypt (A4033) | Decrypt with 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| AES-ECB - Decrypt (A4034) | Decrypt with 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |

© 2026 Cloudlinux Inc., TuxCare division / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| AES-ECB - Decrypt (A4035) | Decrypt with 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| AES-ECB - Decrypt (A4036) | Decrypt with 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| AES-ECB - Decrypt (A4038) | Decrypt with 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| AES-ECB - Decrypt (A4039) | Decrypt with 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| AES-ECB - Decrypt (A4040) | Decrypt with 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| AES-ECB - Decrypt (A4041) | Decrypt with 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| AES-ECB - Decrypt (A4042) | Decrypt with 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |

© 2026 Cloudlinux Inc., TuxCare division / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| AES-ECB - Decrypt (A4043) | Decrypt with 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| AES-XTS Testing Revision 2.0 - Encrypt (A4025) | Encrypt with 128, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-XTS Testing Revision 2.0 - Encrypt (A4032) | Encrypt with 128, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-XTS Testing Revision 2.0 - Encrypt (A4033) | Encrypt with 128, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-XTS Testing Revision 2.0 - Encrypt (A4036) | Encrypt with 128, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-XTS Testing Revision 2.0 - Encrypt (A4038) | Encrypt with 128, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-XTS Testing Revision 2.0 - Encrypt (A4041) | Encrypt with 128, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |

© 2026 Cloudlinux Inc., TuxCare division / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| AES-XTS Testing Revision 2.0 - Decrypt (A4025) | Decrypt with 128, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| AES-XTS Testing Revision 2.0 - Decrypt (A4032) | Decrypt with 128, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| AES-XTS Testing Revision 2.0 - Decrypt (A4033) | Decrypt with 128, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| AES-XTS Testing Revision 2.0 - Decrypt (A4036) | Decrypt with 128, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| AES-XTS Testing Revision 2.0 - Decrypt (A4038) | Decrypt with 128, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| AES-XTS Testing Revision 2.0 - Decrypt (A4041) | Decrypt with 128, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| AES-CBC - Encrypt (A4025) | Encrypt with 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |

© 2026 Cloudlinux Inc., TuxCare division / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| AES-CBC - Encrypt (A4032) | Encrypt with 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-CBC - Encrypt (A4033) | Encrypt with 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-CBC - Encrypt (A4036) | Encrypt with 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-CBC - Encrypt (A4038) | Encrypt with 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-CBC - Encrypt (A4041) | Encrypt with 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-CBC - Decrypt (A4025) | Decrypt with 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| AES-CBC - Decrypt (A4032) | Decrypt with 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |

© 2026 Cloudlinux Inc., TuxCare division / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| AES-CBC - Decrypt (A4033) | Decrypt with 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| AES-CBC - Decrypt (A4036) | Decrypt with 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| AES-CBC - Decrypt (A4038) | Decrypt with 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| AES-CBC - Decrypt (A4041) | Decrypt with 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| AES-CTR - Encrypt (A4025) | Encrypt with 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-CTR - Encrypt (A4032) | Encrypt with 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-CTR - Encrypt (A4033) | Encrypt with 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |

© 2026 Cloudlinux Inc., TuxCare division / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| AES-CTR - Encrypt (A4036) | Encrypt with 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-CTR - Encrypt (A4038) | Encrypt with 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-CTR - Encrypt (A4041) | Encrypt with 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-CTR - Decrypt (A4025) | Decrypt with 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| AES-CTR - Decrypt (A4032) | Decrypt with 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| AES-CTR - Decrypt (A4033) | Decrypt with 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| AES-CTR - Decrypt (A4036) | Decrypt with 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |

© 2026 Cloudlinux Inc., TuxCare division / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| AES-CTR - Decrypt (A4038) | Decrypt with 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| AES-CTR - Decrypt (A4041) | Decrypt with 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| AES-CCM - Encrypt (A4025) | Encrypt with 128, 192, 256 bit keys; 128-bit IVs | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-CCM - Encrypt (A4032) | Encrypt with 128, 192, 256 bit keys; 128-bit IVs | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-CCM - Encrypt (A4033) | Encrypt with 128, 192, 256 bit keys; 128-bit IVs | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-CCM - Encrypt (A4041) | Encrypt with 128, 192, 256 bit keys; 128-bit IVs | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-CCM - Decrypt (A4025) | Decrypt with 128, 192, 256 bit keys; 128-bit IVs | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |

© 2026 Cloudlinux Inc., TuxCare division / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| AES-CCM - Decrypt (A4032) | Decrypt with 128, 192, 256 bit keys; 128-bit IVs | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| AES-CCM - Decrypt (A4033) | Decrypt with 128, 192, 256 bit keys; 128-bit IVs | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| AES-CCM - Decrypt (A4041) | Decrypt with 128, 192, 256 bit keys; 128-bit IVs | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| AES-GCM - Encrypt (A4025) | Encrypt with 128, 192, 256 bit keys; Internal 96-bit IVs | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-GCM - Encrypt (A4030) | Encrypt with 128, 192, 256 bit keys; Internal 96-bit IVs | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-GCM - Encrypt (A4031) | Encrypt with 128, 192, 256 bit keys; Internal 96-bit IVs | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-GCM - Encrypt (A4033) | Encrypt with 128, 192, 256 bit keys; Internal 96-bit IVs | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-GCM - Encrypt (A4034) | Encrypt with 128, 192, 256 bit | KAT | CAST | Module becomes | Encryption | Module initialization |

© 2026 Cloudlinux Inc., TuxCare division / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| | keys; Internal 96-bit IVs | | | operational and services are available for use. | | |
| AES-GCM - Encrypt (A4035) | Encrypt with 128, 192, 256 bit keys; Internal 96-bit IVs | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-GCM - Encrypt (A4038) | Encrypt with 128, 192, 256 bit keys; Internal 96-bit IVs | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-GCM - Encrypt (A4039) | Encrypt with 128, 192, 256 bit keys; Internal 96-bit IVs | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-GCM - Encrypt (A4040) | Encrypt with 128, 192, 256 bit keys; Internal 96-bit IVs | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-GCM - Encrypt (A4041) | Encrypt with 128, 192, 256 bit keys; Internal 96-bit IVs | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-GCM - Encrypt (A4042) | Encrypt with 128, 192, 256 bit keys; Internal 96-bit IVs | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-GCM - Encrypt (A4043) | Encrypt with 128, 192, 256 bit keys; Internal 96-bit IVs | KAT | CAST | Module becomes operational and services | Encryption | Module initialization |

© 2026 Cloudlinux Inc., TuxCare division / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| | | | | are available for use. | | |
| AES-GCM - Decrypt (A4025) | Decrypt with 128, 192, 256 bit keys; external 96-bit IVs | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| AES-GCM - Decrypt (A4030) | Decrypt with 128, 192, 256 bit keys; external 96-bit IVs | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| AES-GCM - Decrypt (A4031) | Decrypt with 128, 192, 256 bit keys; external 96-bit IVs | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| AES-GCM - Decrypt (A4033) | Decrypt with 128, 192, 256 bit keys; external 96-bit IVs | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| AES-GCM - Decrypt (A4034) | Decrypt with 128, 192, 256 bit keys; external 96-bit IVs | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| AES-GCM - Decrypt (A4035) | Decrypt with 128, 192, 256 bit keys; external 96-bit IVs | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| AES-GCM - Decrypt (A4038) | Decrypt with 128, 192, 256 bit keys; external 96-bit IVs | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |

© 2026 Cloudlinux Inc., TuxCare division / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| AES-GCM - Decrypt (A4039) | Decrypt with 128, 192, 256 bit keys; external 96-bit IVs | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| AES-GCM - Decrypt (A4040) | Decrypt with 128, 192, 256 bit keys; external 96-bit IVs | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| AES-GCM - Decrypt (A4041) | Decrypt with 128, 192, 256 bit keys; external 96-bit IVs | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| AES-GCM - Decrypt (A4042) | Decrypt with 128, 192, 256 bit keys; external 96-bit IVs | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| AES-GCM - Decrypt (A4043) | Decrypt with 128, 192, 256 bit keys; external 96-bit IVs | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| AES-CMAC - Encrypt (A4025) | Encrypt with 128 and 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Message authentication | Module initialization |
| AES-CMAC - Encrypt (A4032) | Encrypt with 128 and 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Message authentication | Module initialization |
| AES-CMAC - Encrypt (A4033) | Encrypt with 128 and 256 bit keys | KAT | CAST | Module becomes | Message authentication | Module initialization |

© 2026 Cloudlinux Inc., TuxCare division / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| | | | | operational and services are available for use. | | |
| AES-CMAC - Encrypt (A4041) | Encrypt with 128 and 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Message authentication | Module initialization |
| AES-CMAC - Decrypt(A4025) | Decrypt with 128 and 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Message authentication | Module initialization |
| AES-CMAC - Decrypt (A4032) | Decrypt with 128 and 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Message authentication | Module initialization |
| AES-CMAC - Decrypt (A4033) | Decrypt with 128 and 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Message authentication | Module initialization |
| AES-CMAC - Decrypt (A4041) | Decrypt with 128 and 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Message authentication | Module initialization |
| HMAC-SHA2-224 (A4025) | SHA2-224, 32-1048 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Message authentication | Module initialization |
| HMAC-SHA2-224 (A4032) | SHA2-224, 32-1048 bit keys | KAT | CAST | Module becomes operational and services | Message authentication | Module initialization |

© 2026 Cloudlinux Inc., TuxCare division / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| | | | | are available for use. | | |
| HMAC-SHA2-224 (A4036) | SHA2-224, 32-1048 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Message authentication | Module initialization |
| HMAC-SHA2-224 (A4037) | SHA2-224, 32-1048 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Message authentication | Module initialization |
| HMAC-SHA2-224 (A4047) | SHA2-224, 32-1048 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Message authentication | Module initialization |
| HMAC-SHA2-224 (A4048) | SHA2-224, 32-1048 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Message authentication | Module initialization |
| HMAC-SHA2-224 (A4049) | SHA2-224, 32-1048 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Message authentication | Module initialization |
| HMAC-SHA2-256 (A4025) | SHA2-256, 32-64 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Message authentication | Module initialization |
| HMAC-SHA2-256 (A4032) | SHA2-256, 32-64 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Message authentication | Module initialization |

© 2026 Cloudlinux Inc., TuxCare division / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| HMAC-SHA2-256 (A4036) | SHA2-256, 32-64 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Message authentication | Module initialization |
| HMAC-SHA2-256 (A4037) | SHA2-256, 32-64 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Message authentication | Module initialization |
| HMAC-SHA2-256 (A4047) | SHA2-256, 32-64 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Message authentication | Module initialization |
| HMAC-SHA2-256 (A4048) | SHA2-256, 32-64 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Message authentication | Module initialization |
| HMAC-SHA2-256 (A4049) | SHA2-256, 32-64 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Message authentication | Module initialization |
| HMAC-SHA2-384 (A4025) | SHA2-384, 32-1048 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Message authentication | Module initialization |
| HMAC-SHA2-384 (A4047) | SHA2-384, 32-1048 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Message authentication | Module initialization |
| HMAC-SHA2-384 (A4048) | SHA2-384, 32-1048 bit keys | KAT | CAST | Module becomes | Message authentication | Module initialization |

© 2026 Cloudlinux Inc., TuxCare division / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| | | | | operational and services are available for use. | | |
| HMAC-SHA2-384 (A4049) | SHA2-384, 32-1048 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Message authentication | Module initialization |
| HMAC-SHA2-512 (A4025) | SHA2-512, 32-1048 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Message authentication | Module initialization. Before integrity test. |
| HMAC-SHA2-512 (A4047) | SHA2-512, 32-1048 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Message authentication | Module initialization. Before integrity test. |
| HMAC-SHA2-512 (A4048) | SHA2-512, 32-1048 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Message authentication | Module initialization. Before integrity test. |
| HMAC-SHA2-512 (A4049) | SHA2-512, 32-1048 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Message authentication | Module initialization. Before integrity test. |
| Counter DRBG (A4025) | 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 (A4030) | 128, 192, 256 bit keys With/without | KAT | CAST | Module becomes operational | Seed, Generate | Module initialization |

© 2026 Cloudlinux Inc., TuxCare division / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

| 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 (A4031) | 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 (A4033) | 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 (A4034) | 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 (A4035) | 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 (A4038) | 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 (A4039) | 128, 192, 256 bit keys With/without PR; Health test per section 11.3 | KAT | CAST | Module becomes operational and services | Seed, Generate | Module initialization |

© 2026 Cloudlinux Inc., TuxCare division / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| | of SP 800-90Arev1 | | | are available for use. | | |
| Counter DRBG (A4040) | 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 (A4041) | 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 (A4042) | 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 (A4043) | 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 (A4025) | 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 (A4030) | 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 (A4031) | SHA-256 With/without | KAT | CAST | Module becomes | Seed, Generate | Module initialization |

© 2026 Cloudlinux Inc., TuxCare division / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| | PR; Health test per section 11.3 of SP 800-90Arev1 | | | operational and services are available for use. | | |
| Hash DRBG (A4034) | 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 (A4035) | 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 (A4038) | 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 (A4039) | 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 (A4040) | 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 (A4041) | 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 (A4042) | SHA-256 With/without PR; Health test per section 11.3 | KAT | CAST | Module becomes operational and services | Seed, Generate | Module initialization |

© 2026 Cloudlinux Inc., TuxCare division / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| | of SP 800-90Arev1 | | | are available for use. | | |
| Hash DRBG (A4043) | 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 (A4047) | 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 (A4048) | 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 (A4049) | 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 (A4025) | HMAC-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 (A4030) | HMAC-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 (A4031) | HMAC-SHA-256, SHA512 With/without PR; Health test | KAT | CAST | Module becomes operational and services | Seed, Generate | Module initialization |

© 2026 Cloudlinux Inc., TuxCare division / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| | per section 11.3 of SP 800-90Arev1 | | | are available for use. | | |
| HMAC DRBG (A4034) | HMAC-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 (A4035) | HMAC-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 (A4038) | HMAC-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 (A4039) | HMAC-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 (A4040) | HMAC-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 (A4041) | HMAC-SHA-256, SHA512 With/without PR; Health test per section 11.3 | KAT | CAST | Module becomes operational and services are available for use. | Seed, Generate | Module initialization |

© 2026 Cloudlinux Inc., TuxCare division / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| | of SP 800-90Arev1 | | | | | |
| HMAC DRBG (A4042) | HMAC-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 (A4043) | HMAC-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 (A4047) | HMAC-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 (A4048) | HMAC-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 (A4049) | HMAC-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 |
| RSA SigVer (FIPS186-4) (A4025) | 4096-bit key with SHA-256 | KAT | CAST | Module becomes operational and services are available for use. | Signature verification | Module initialization. Before integrity test. |

© 2026 Cloudlinux Inc., TuxCare division / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| RSA SigVer (FIPS186-4) (A4047) | 4096-bit key with SHA-256 | KAT | CAST | Module becomes operational and services are available for use. | Signature verification | Module initialization. Before integrity test. |
| RSA SigVer (FIPS186-4) (A4048) | 4096-bit key with SHA-256 | KAT | CAST | Module becomes operational and services are available for use. | Signature verification | Module initialization. Before integrity test. |
| RSA SigVer (FIPS186-4) (A4049) | 4096-bit key with SHA-256 | KAT | CAST | Module becomes operational and services are available for use. | Signature verification | Module initialization. Before integrity test. |
| SHA3-224 (A4026) | 0-8184 bit messages | KAT | CAST | Module becomes operational and services are available for use. | Message digest | Module initialization |
| SHA3-256 (A4026) | 0-8184 bit messages | KAT | CAST | Module becomes operational and services are available for use. | Message digest | Module initialization |
| SHA3-384 (A4026) | 0-8184 bit messages | KAT | CAST | Module becomes operational and services are available for use. | Message digest | Module initialization |
| SHA3-512 (A4026) | 0-8184 bit messages | KAT | CAST | Module becomes operational and services are available for use. | Message digest | Module initialization |
| HMAC-SHA3-224 (A4026) | SHA3-224, 32-1048 bit keys | KAT | CAST | Module becomes | Message authentication | Module initialization |

© 2026 Cloudlinux Inc., TuxCare division / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| | | | | operational and services are available for use. | | |
| HMAC-SHA3-256 (A4026) | SHA3-256, 32-1048 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Message authentication | Module initialization |
| HMAC-SHA3-384 (A4026) | SHA3-384, 32-1048 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Message authentication | Module initialization |
| HMAC-SHA3-512 (A4026) | SHA3-512, 32-1048 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Message authentication | Module initialization |
| AES-CFB128 - Encrypt (A4027) | Encrypt with 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-CFB128 - Encrypt (A4033) | Encrypt with 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-CFB128 - Encrypt (A4044) | Encrypt with 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-CFB128 - Decrypt (A4027) | Decrypt with 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services | Decryption | Module initialization |

© 2026 Cloudlinux Inc., TuxCare division / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| | | | | are available for use. | | |
| AES-CFB128 - Decrypt (A4033) | Decrypt with 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| AES-CFB128 - Decrypt (A4044) | Decrypt with 128, 192, 256 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| AES-CBC-CS3 - Encrypt (A4029) | Encrypt with 128 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-CBC-CS3 - Encrypt (A4032) | Encrypt with 128 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-CBC-CS3 - Encrypt (A4033) | Encrypt with 128 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-CBC-CS3 - Encrypt (A4046) | Encrypt with 128 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-CBC-CS3 - Decrypt (A4029) | Decrypt with 128 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |

© 2026 Cloudlinux Inc., TuxCare division / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| AES-CBC-CS3 - Decrypt (A4032) | Decrypt with 128 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| AES-CBC-CS3 - Decrypt (A4033) | Decrypt with 128 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| AES-CBC-CS3 - Decrypt (A4046) | Decrypt with 128 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| AES-OFB - Encrypt (A4028) | 128 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-OFB - Encrypt (A4033) | 128 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-OFB - Encrypt (A4045) | 128 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Encryption | Module initialization |
| AES-OFB - Decrypt (A4028) | 128 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| AES-OFB - Decrypt (A4033) | 128 bit keys | KAT | CAST | Module becomes | Decryption | Module initialization |

© 2026 Cloudlinux Inc., TuxCare division / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| | | | | operational and services are available for use. | | |
| AES-OFB - Decrypt (A4045) | 128 bit keys | KAT | CAST | Module becomes operational and services are available for use. | Decryption | Module initialization |
| Entropy Source RCT startup | 1024 samples | RCT | CAST | Module becomes operational and services are available for use. | Entropy source start-up test | Entropy source initialization |
| Entropy Source APT startup | 1024 samples | APT | CAST | Module becomes operational and services are available for use. | Entropy source start-up test | Entropy source initialization |
| Entropy Source RCT Continuous | Cutoff C = 61 | RCT | CAST | Entropy source is operational | Entropy source continuous test | Continuously |
| Entropy Source APT Continuous | Cutoff C = 355 | APT | CAST | Entropy source is operational | Entropy source continuous test | Continuously |

*Table 20: Conditional Self-Tests*

When all of the pre-operational self-tests pass successfully, the module automatically performs all cryptographic algorithm self-tests (CASTs) as specified in Table "Conditional Self-Tests". Only if these CASTs also passed successfully, the module transitions to the operational state. No operator intervention is required to reach this point. Services are not available, and data output (via the data output interface) is inhibited during the 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 (A4025) | Message Authentication | SW/FW Integrity | On demand | Manually |
| HMAC-SHA2-512 (A4047) | Message Authentication | SW/FW Integrity | On demand | Manually |

© 2026 Cloudlinux Inc., TuxCare division / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

| Algorithm or Test | Test Method | Test Type | Period | Periodic Method |
|---|---|---|---|---|
| HMAC-SHA2-512 (A4048) | Message Authentication | SW/FW Integrity | On demand | Manually |
| HMAC-SHA2-512 (A4049) | Message Authentication | SW/FW Integrity | On demand | Manually |
| RSA SigVer (FIPS186-4) (A4025) | Signature Verification | SW/FW Integrity | On demand | Manually |
| RSA SigVer (FIPS186-4) (A4047) | Signature Verification | SW/FW Integrity | On demand | Manually |
| RSA SigVer (FIPS186-4) (A4048) | Signature Verification | SW/FW Integrity | On demand | Manually |
| RSA SigVer (FIPS186-4) (A4049) | Signature Verification | SW/FW Integrity | On demand | Manually |

*Table 21: Pre-Operational Periodic Information*

| Algorithm or Test | Test Method | Test Type | Period | Periodic Method |
|---|---|---|---|---|
| SHA2-224 (A4025) | KAT | CAST | On demand | Manually |
| SHA2-224 (A4032) | KAT | CAST | On demand | Manually |
| SHA2-224 (A4036) | KAT | CAST | On demand | Manually |
| SHA2-224 (A4037) | KAT | CAST | On demand | Manually |
| SHA2-224 (A4047) | KAT | CAST | On demand | Manually |
| SHA2-224 (A4048) | KAT | CAST | On demand | Manually |
| SHA2-224 (A4049) | KAT | CAST | On demand | Manually |
| SHA2-256 (A4025) | KAT | CAST | On demand | Manually |
| SHA2-256 (A4032) | KAT | CAST | On demand | Manually |
| SHA2-256 (A4036) | KAT | CAST | On demand | Manually |
| SHA2-256 (A4037) | KAT | CAST | On demand | Manually |
| SHA2-256 (A4047) | KAT | CAST | On demand | Manually |
| SHA2-256 (A4048) | KAT | CAST | On demand | Manually |
| SHA2-256 (A4049) | KAT | CAST | On demand | Manually |
| SHA2-384 (A4025) | KAT | CAST | On demand | Manually |
| SHA2-384 (A4047) | KAT | CAST | On demand | Manually |
| SHA2-384 (A4048) | KAT | CAST | On demand | Manually |
| SHA2-384 (A4049) | KAT | CAST | On demand | Manually |
| SHA2-512 (A4025) | KAT | CAST | On demand | Manually |
| SHA2-512 (A4047) | KAT | CAST | On demand | Manually |
| SHA2-512 (A4048) | KAT | CAST | On demand | Manually |
| SHA2-512 (A4049) | KAT | CAST | On demand | Manually |
| AES-ECB - Encrypt (A4025) | KAT | CAST | On demand | Manually |

© 2026 Cloudlinux Inc., TuxCare division / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

| Algorithm or Test | Test Method | Test Type | Period | Periodic Method |
|---|---|---|---|---|
| AES-ECB - Encrypt (A4030) | KAT | CAST | On demand | Manually |
| AES-ECB - Encrypt (A4031) | KAT | CAST | On demand | Manually |
| AES-ECB - Encrypt (A4032) | KAT | CAST | On demand | Manually |
| AES-ECB - Encrypt (A4033) | KAT | CAST | On demand | Manually |
| AES-ECB - Encrypt (A4034) | KAT | CAST | On demand | Manually |
| AES-ECB - Encrypt (A4035) | KAT | CAST | On demand | Manually |
| AES-ECB - Encrypt (A4036) | KAT | CAST | On demand | Manually |
| AES-ECB - Encrypt (A4038) | KAT | CAST | On demand | Manually |
| AES-ECB - Encrypt (A4039) | KAT | CAST | On demand | Manually |
| AES-ECB - Encrypt (A4040) | KAT | CAST | On demand | Manually |
| AES-ECB - Encrypt (A4041) | KAT | CAST | On demand | Manually |
| AES-ECB - Encrypt (A4042) | KAT | CAST | On demand | Manually |
| AES-ECB - Encrypt (A4043) | KAT | CAST | On demand | Manually |
| AES-ECB - Decrypt (A4025) | KAT | CAST | On demand | Manually |
| AES-ECB - Decrypt (A4030) | KAT | CAST | On demand | Manually |
| AES-ECB - Decrypt (A4031) | KAT | CAST | On demand | Manually |
| AES-ECB - Decrypt (A4032) | KAT | CAST | On demand | Manually |
| AES-ECB - Decrypt (A4033) | KAT | CAST | On demand | Manually |
| AES-ECB - Decrypt (A4034) | KAT | CAST | On demand | Manually |
| AES-ECB - Decrypt (A4035) | KAT | CAST | On demand | Manually |
| AES-ECB - Decrypt (A4036) | KAT | CAST | On demand | Manually |
| AES-ECB - Decrypt (A4038) | KAT | CAST | On demand | Manually |

© 2026 Cloudlinux Inc., TuxCare division / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

| Algorithm or Test | Test Method | Test Type | Period | Periodic Method |
|---|---|---|---|---|
| AES-ECB - Decrypt (A4039) | KAT | CAST | On demand | Manually |
| AES-ECB - Decrypt (A4040) | KAT | CAST | On demand | Manually |
| AES-ECB - Decrypt (A4041) | KAT | CAST | On demand | Manually |
| AES-ECB - Decrypt (A4042) | KAT | CAST | On demand | Manually |
| AES-ECB - Decrypt (A4043) | KAT | CAST | On demand | Manually |
| AES-XTS Testing Revision 2.0 - Encrypt (A4025) | KAT | CAST | On demand | Manually |
| AES-XTS Testing Revision 2.0 - Encrypt (A4032) | KAT | CAST | On demand | Manually |
| AES-XTS Testing Revision 2.0 - Encrypt (A4033) | KAT | CAST | On demand | Manually |
| AES-XTS Testing Revision 2.0 - Encrypt (A4036) | KAT | CAST | On demand | Manually |
| AES-XTS Testing Revision 2.0 - Encrypt (A4038) | KAT | CAST | On demand | Manually |
| AES-XTS Testing Revision 2.0 - Encrypt (A4041) | KAT | CAST | On demand | Manually |
| AES-XTS Testing Revision 2.0 - Decrypt (A4025) | KAT | CAST | On demand | Manually |
| AES-XTS Testing Revision 2.0 - Decrypt (A4032) | KAT | CAST | On demand | Manually |
| AES-XTS Testing Revision 2.0 - Decrypt (A4033) | KAT | CAST | On demand | Manually |
| AES-XTS Testing Revision 2.0 - Decrypt (A4036) | KAT | CAST | On demand | Manually |
| AES-XTS Testing Revision 2.0 - Decrypt (A4038) | KAT | CAST | On demand | Manually |

© 2026 Cloudlinux Inc., TuxCare division / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

| Algorithm or Test | Test Method | Test Type | Period | Periodic Method |
|---|---|---|---|---|
| AES-XTS Testing Revision 2.0 - Decrypt (A4041) | KAT | CAST | On demand | Manually |
| AES-CBC - Encrypt (A4025) | KAT | CAST | On demand | Manually |
| AES-CBC - Encrypt (A4032) | KAT | CAST | On demand | Manually |
| AES-CBC - Encrypt (A4033) | KAT | CAST | On demand | Manually |
| AES-CBC - Encrypt (A4036) | KAT | CAST | On demand | Manually |
| AES-CBC - Encrypt (A4038) | KAT | CAST | On demand | Manually |
| AES-CBC - Encrypt (A4041) | KAT | CAST | On demand | Manually |
| AES-CBC - Decrypt (A4025) | KAT | CAST | On demand | Manually |
| AES-CBC - Decrypt (A4032) | KAT | CAST | On demand | Manually |
| AES-CBC - Decrypt (A4033) | KAT | CAST | On demand | Manually |
| AES-CBC - Decrypt (A4036) | KAT | CAST | On demand | Manually |
| AES-CBC - Decrypt (A4038) | KAT | CAST | On demand | Manually |
| AES-CBC - Decrypt (A4041) | KAT | CAST | On demand | Manually |
| AES-CTR - Encrypt (A4025) | KAT | CAST | On demand | Manually |
| AES-CTR - Encrypt (A4032) | KAT | CAST | On demand | Manually |
| AES-CTR - Encrypt (A4033) | KAT | CAST | On demand | Manually |
| AES-CTR - Encrypt (A4036) | KAT | CAST | On demand | Manually |
| AES-CTR - Encrypt (A4038) | KAT | CAST | On demand | Manually |
| AES-CTR - Encrypt (A4041) | KAT | CAST | On demand | Manually |
| AES-CTR - Decrypt (A4025) | KAT | CAST | On demand | Manually |
| AES-CTR - Decrypt (A4032) | KAT | CAST | On demand | Manually |

© 2026 Cloudlinux Inc., TuxCare division / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

| Algorithm or Test | Test Method | Test Type | Period | Periodic Method |
|---|---|---|---|---|
| AES-CTR - Decrypt (A4033) | KAT | CAST | On demand | Manually |
| AES-CTR - Decrypt (A4036) | KAT | CAST | On demand | Manually |
| AES-CTR - Decrypt (A4038) | KAT | CAST | On demand | Manually |
| AES-CTR - Decrypt (A4041) | KAT | CAST | On demand | Manually |
| AES-CCM - Encrypt (A4025) | KAT | CAST | On demand | Manually |
| AES-CCM - Encrypt (A4032) | KAT | CAST | On demand | Manually |
| AES-CCM - Encrypt (A4033) | KAT | CAST | On demand | Manually |
| AES-CCM - Encrypt (A4041) | KAT | CAST | On demand | Manually |
| AES-CCM - Decrypt (A4025) | KAT | CAST | On demand | Manually |
| AES-CCM - Decrypt (A4032) | KAT | CAST | On demand | Manually |
| AES-CCM - Decrypt (A4033) | KAT | CAST | On demand | Manually |
| AES-CCM - Decrypt (A4041) | KAT | CAST | On demand | Manually |
| AES-GCM - Encrypt (A4025) | KAT | CAST | On demand | Manually |
| AES-GCM - Encrypt (A4030) | KAT | CAST | On demand | Manually |
| AES-GCM - Encrypt (A4031) | KAT | CAST | On demand | Manually |
| AES-GCM - Encrypt (A4033) | KAT | CAST | On demand | Manually |
| AES-GCM - Encrypt (A4034) | KAT | CAST | On demand | Manually |
| AES-GCM - Encrypt (A4035) | KAT | CAST | On demand | Manually |
| AES-GCM - Encrypt (A4038) | KAT | CAST | On demand | Manually |
| AES-GCM - Encrypt (A4039) | KAT | CAST | On demand | Manually |
| AES-GCM - Encrypt (A4040) | KAT | CAST | On demand | Manually |
| AES-GCM - Encrypt (A4041) | KAT | CAST | On demand | Manually |

© 2026 Cloudlinux Inc., TuxCare division / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

| Algorithm or Test | Test Method | Test Type | Period | Periodic Method |
|---|---|---|---|---|
| AES-GCM - Encrypt (A4042) | KAT | CAST | On demand | Manually |
| AES-GCM - Encrypt (A4043) | KAT | CAST | On demand | Manually |
| AES-GCM - Decrypt (A4025) | KAT | CAST | On demand | Manually |
| AES-GCM - Decrypt (A4030) | KAT | CAST | On demand | Manually |
| AES-GCM - Decrypt (A4031) | KAT | CAST | On demand | Manually |
| AES-GCM - Decrypt (A4033) | KAT | CAST | On demand | Manually |
| AES-GCM - Decrypt (A4034) | KAT | CAST | On demand | Manually |
| AES-GCM - Decrypt (A4035) | KAT | CAST | On demand | Manually |
| AES-GCM - Decrypt (A4038) | KAT | CAST | On demand | Manually |
| AES-GCM - Decrypt (A4039) | KAT | CAST | On demand | Manually |
| AES-GCM - Decrypt (A4040) | KAT | CAST | On demand | Manually |
| AES-GCM - Decrypt (A4041) | KAT | CAST | On demand | Manually |
| AES-GCM - Decrypt (A4042) | KAT | CAST | On demand | Manually |
| AES-GCM - Decrypt (A4043) | KAT | CAST | On demand | Manually |
| AES-CMAC - Encrypt (A4025) | KAT | CAST | On demand | Manually |
| AES-CMAC - Encrypt (A4032) | KAT | CAST | On demand | Manually |
| AES-CMAC - Encrypt (A4033) | KAT | CAST | On demand | Manually |
| AES-CMAC - Encrypt (A4041) | KAT | CAST | On demand | Manually |
| AES-CMAC - Decrypt(A4025) | KAT | CAST | On demand | Manually |
| AES-CMAC - Decrypt (A4032) | KAT | CAST | On demand | Manually |
| AES-CMAC - Decrypt (A4033) | KAT | CAST | On demand | Manually |
| AES-CMAC - Decrypt (A4041) | KAT | CAST | On demand | Manually |

© 2026 Cloudlinux Inc., TuxCare division / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

| Algorithm or Test | Test Method | Test Type | Period | Periodic Method |
|---|---|---|---|---|
| HMAC-SHA2-224 (A4025) | KAT | CAST | On demand | Manually |
| HMAC-SHA2-224 (A4032) | KAT | CAST | On demand | Manually |
| HMAC-SHA2-224 (A4036) | KAT | CAST | On demand | Manually |
| HMAC-SHA2-224 (A4037) | KAT | CAST | On demand | Manually |
| HMAC-SHA2-224 (A4047) | KAT | CAST | On demand | Manually |
| HMAC-SHA2-224 (A4048) | KAT | CAST | On demand | Manually |
| HMAC-SHA2-224 (A4049) | KAT | CAST | On demand | Manually |
| HMAC-SHA2-256 (A4025) | KAT | CAST | On demand | Manually |
| HMAC-SHA2-256 (A4032) | KAT | CAST | On demand | Manually |
| HMAC-SHA2-256 (A4036) | KAT | CAST | On demand | Manually |
| HMAC-SHA2-256 (A4037) | KAT | CAST | On demand | Manually |
| HMAC-SHA2-256 (A4047) | KAT | CAST | On demand | Manually |
| HMAC-SHA2-256 (A4048) | KAT | CAST | On demand | Manually |
| HMAC-SHA2-256 (A4049) | KAT | CAST | On demand | Manually |
| HMAC-SHA2-384 (A4025) | KAT | CAST | On demand | Manually |
| HMAC-SHA2-384 (A4047) | KAT | CAST | On demand | Manually |
| HMAC-SHA2-384 (A4048) | KAT | CAST | On demand | Manually |
| HMAC-SHA2-384 (A4049) | KAT | CAST | On demand | Manually |
| HMAC-SHA2-512 (A4025) | KAT | CAST | On demand | Manually |
| HMAC-SHA2-512 (A4047) | KAT | CAST | On demand | Manually |
| HMAC-SHA2-512 (A4048) | KAT | CAST | On demand | Manually |
| HMAC-SHA2-512 (A4049) | KAT | CAST | On demand | Manually |

© 2026 Cloudlinux Inc., TuxCare division / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

| Algorithm or Test | Test Method | Test Type | Period | Periodic Method |
|---|---|---|---|---|
| Counter DRBG (A4025) | KAT | CAST | On demand | Manually |
| Counter DRBG (A4030) | KAT | CAST | On demand | Manually |
| Counter DRBG (A4031) | KAT | CAST | On demand | Manually |
| Counter DRBG (A4033) | KAT | CAST | On demand | Manually |
| Counter DRBG (A4034) | KAT | CAST | On demand | Manually |
| Counter DRBG (A4035) | KAT | CAST | On demand | Manually |
| Counter DRBG (A4038) | KAT | CAST | On demand | Manually |
| Counter DRBG (A4039) | KAT | CAST | On demand | Manually |
| Counter DRBG (A4040) | KAT | CAST | On demand | Manually |
| Counter DRBG (A4041) | KAT | CAST | On demand | Manually |
| Counter DRBG (A4042) | KAT | CAST | On demand | Manually |
| Counter DRBG (A4043) | KAT | CAST | On demand | Manually |
| Hash DRBG (A4025) | KAT | CAST | On demand | Manually |
| Hash DRBG (A4030) | KAT | CAST | On demand | Manually |
| Hash DRBG (A4031) | KAT | CAST | On demand | Manually |
| Hash DRBG (A4034) | KAT | CAST | On demand | Manually |
| Hash DRBG (A4035) | KAT | CAST | On demand | Manually |
| Hash DRBG (A4038) | KAT | CAST | On demand | Manually |
| Hash DRBG (A4039) | KAT | CAST | On demand | Manually |
| Hash DRBG (A4040) | KAT | CAST | On demand | Manually |
| Hash DRBG (A4041) | KAT | CAST | On demand | Manually |
| Hash DRBG (A4042) | KAT | CAST | On demand | Manually |

© 2026 Cloudlinux Inc., TuxCare division / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

| Algorithm or Test | Test Method | Test Type | Period | Periodic Method |
|---|---|---|---|---|
| Hash DRBG (A4043) | KAT | CAST | On demand | Manually |
| Hash DRBG (A4047) | KAT | CAST | On demand | Manually |
| Hash DRBG (A4048) | KAT | CAST | On demand | Manually |
| Hash DRBG (A4049) | KAT | CAST | On demand | Manually |
| HMAC DRBG (A4025) | KAT | CAST | On demand | Manually |
| HMAC DRBG (A4030) | KAT | CAST | On demand | Manually |
| HMAC DRBG (A4031) | KAT | CAST | On demand | Manually |
| HMAC DRBG (A4034) | KAT | CAST | On demand | Manually |
| HMAC DRBG (A4035) | KAT | CAST | On demand | Manually |
| HMAC DRBG (A4038) | KAT | CAST | On demand | Manually |
| HMAC DRBG (A4039) | KAT | CAST | On demand | Manually |
| HMAC DRBG (A4040) | KAT | CAST | On demand | Manually |
| HMAC DRBG (A4041) | KAT | CAST | On demand | Manually |
| HMAC DRBG (A4042) | KAT | CAST | On demand | Manually |
| HMAC DRBG (A4043) | KAT | CAST | On demand | Manually |
| HMAC DRBG (A4047) | KAT | CAST | On demand | Manually |
| HMAC DRBG (A4048) | KAT | CAST | On demand | Manually |
| HMAC DRBG (A4049) | KAT | CAST | On demand | Manually |
| RSA SigVer (FIPS186-4) (A4025) | KAT | CAST | On demand | Manually |
| RSA SigVer (FIPS186-4) (A4047) | KAT | CAST | On demand | Manually |

© 2026 Cloudlinux Inc., TuxCare division / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

| Algorithm or Test | Test Method | Test Type | Period | Periodic Method |
|---|---|---|---|---|
| RSA SigVer (FIPS186-4) (A4048) | KAT | CAST | On demand | Manually |
| RSA SigVer (FIPS186-4) (A4049) | KAT | CAST | On demand | Manually |
| SHA3-224 (A4026) | KAT | CAST | On demand | Manually |
| SHA3-256 (A4026) | KAT | CAST | On demand | Manually |
| SHA3-384 (A4026) | KAT | CAST | On demand | Manually |
| SHA3-512 (A4026) | KAT | CAST | On demand | Manually |
| HMAC-SHA3-224 (A4026) | KAT | CAST | On demand | Manually |
| HMAC-SHA3-256 (A4026) | KAT | CAST | On demand | Manually |
| HMAC-SHA3-384 (A4026) | KAT | CAST | On demand | Manually |
| HMAC-SHA3-512 (A4026) | KAT | CAST | On demand | Manually |
| AES-CFB128 - Encrypt (A4027) | KAT | CAST | On demand | Manually |
| AES-CFB128 - Encrypt (A4033) | KAT | CAST | On demand | Manually |
| AES-CFB128 - Encrypt (A4044) | KAT | CAST | On demand | Manually |
| AES-CFB128 - Decrypt (A4027) | KAT | CAST | On demand | Manually |
| AES-CFB128 - Decrypt (A4033) | KAT | CAST | On demand | Manually |
| AES-CFB128 - Decrypt (A4044) | KAT | CAST | On demand | Manually |
| AES-CBC-CS3 - Encrypt (A4029) | KAT | CAST | On demand | Manually |
| AES-CBC-CS3 - Encrypt (A4032) | KAT | CAST | On demand | Manually |
| AES-CBC-CS3 - Encrypt (A4033) | KAT | CAST | On demand | Manually |
| AES-CBC-CS3 - Encrypt (A4046) | KAT | CAST | On demand | Manually |
| AES-CBC-CS3 - Decrypt (A4029) | KAT | CAST | On demand | Manually |
| AES-CBC-CS3 - Decrypt (A4032) | KAT | CAST | On demand | Manually |
| AES-CBC-CS3 - Decrypt (A4033) | KAT | CAST | On demand | Manually |

© 2026 Cloudlinux Inc., TuxCare division / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

| Algorithm or Test | Test Method | Test Type | Period | Periodic Method |
|---|---|---|---|---|
| AES-CBC-CS3 - Decrypt (A4046) | KAT | CAST | On demand | Manually |
| AES-OFB - Encrypt (A4028) | KAT | CAST | On demand | Manually |
| AES-OFB - Encrypt (A4033) | KAT | CAST | On demand | Manually |
| AES-OFB - Encrypt (A4045) | KAT | CAST | On demand | Manually |
| AES-OFB - Decrypt (A4028) | KAT | CAST | On demand | Manually |
| AES-OFB - Decrypt (A4033) | KAT | CAST | On demand | Manually |
| AES-OFB - Decrypt (A4045) | KAT | CAST | On demand | Manually |
| Entropy Source RCT startup | RCT | CAST | On demand | Manually |
| Entropy Source APT startup | APT | CAST | On demand | Manually |
| Entropy Source RCT Continuous | RCT | CAST | On demand | Manually |
| Entropy Source APT Continuous | APT | CAST | On demand | Manually |

*Table 22: Conditional Periodic Information*

The module does not implement any periodic self-tests.

## 10.4 Error States

| Name | Description | Conditions | Recovery Method | Indicator |
|---|---|---|---|---|
| Error | The Linux kernel immediately stops executing | Software integrity test failure<br>CAST failure | Restart of the module | Kernel Panic |

*Table 23: 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

The software integrity tests, cryptographic algorithm self-tests, and entropy source start-up tests can be invoked on demand by unloading and subsequently re-initializing the module.

© 2026 Cloudlinux Inc., TuxCare division / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

# 11 Life-Cycle Assurance

## 11.1 Installation, Initialization, and Startup Procedures

The module is distributed as a part of the AlmaLinux 9.2 package in the form of the kernel-5.14.0-284.1101.el9_2.tuxcare.11, libkcapi-1.3.1-3.el9, and libkcapi-hmaccalc-1.3.1-3.el9 RPM packages.
Before the packages are installed, the AlmaLinux 9.2 system must operate in approved mode. This can be achieved by:

- Starting the installation in approved mode. 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.
- Switching the system into approved mode after the installation. Execute the *fips-mode-setup --enable* command. Restart the system.

In both cases, the Crypto Officer must verify the AlmaLinux 9.2 system operates in approved mode by executing the *fips-mode-setup --check* command, which should output "FIPS mode is enabled."

After installation of the kernel-5.14.0-284.1101.el9_2.tuxcare.11, libkcapi-1.3.1-3.el9, and libkcapi-hmaccalc-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:

*Kernel Cryptography module for AlmaLinux 9*

Then, the Crypto Officer must execute the *cat /proc/sys/crypto/fips_version* and *rpm -q libkcapi* commands. These commands must output the following (one line per output) depending on the platform in which are executed:

Intel:

*5.14.0-284.1101.el9_2.tuxcare.11.x86_64*
*libkcapi-1.3.1-3.el9.x86_64*

ARM:

*5.14.0-284.1101.el9_2.tuxcare.11.aarch64*
*libkcapi-1.3.1-3.el9.aarch64*

## 11.2 Administrator Guidance

The cryptographic boundary consists only of those APIs provided by the Kernel crypto API. If any other API in the Linux kernel is invoked, the user is not interacting with the module specified in this Security Policy.

## 11.3 Non-Administrator Guidance

There is no non-administrator guidance.

© 2026 Cloudlinux Inc., TuxCare division / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

## 11.5 End of Life

Secure disposal is the customer's responsibility, since the module goes EOL with the operating system.

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-5.14.0-284.1101.el9_2.tuxcare.11, libkcapi-1.3.1-3.el9, and libkcapi-hmaccalc-1.3.1-3.el9 RPM packages (for both Intel and ARM platforms) can be uninstalled from the AlmaLinux 9.2 system.

© 2026 Cloudlinux Inc., TuxCare division / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

# 12 Mitigation of Other Attacks

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

© 2026 Cloudlinux Inc., TuxCare division / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

# 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 |
| CTS | Ciphertext Stealing |
| DRBG | Deterministic Random Bit Generator |
| ECB | Electronic Code Book |
| ESV | Entropy Source Validation |
| FIPS | Federal Information Processing Standards |
| GCM | Galois Counter Mode |
| GMAC | Galois Counter Mode Message Authentication Code |
| HKDF | HMAC-based Key Derivation Function |
| HMAC | Keyed-Hash Message Authentication Code |
| IPsec | Internet Protocol Security |
| KAT | Known Answer Test |
| KBKDF | Key-based Key Derivation Function |
| MAC | Message Authentication Code |
| NIST | National Institute of Science and Technology |
| PAA | Processor Algorithm Acceleration |
| PCT | Pair-wise Consistency Test |
| PBKDF2 | Password-based Key Derivation Function v2 |
| 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 |

© 2026 Cloudlinux Inc., TuxCare division / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

# Appendix B. References


| | |
|---|---|
| FIPS 140-3 | FIPS PUB 140-3 - Security Requirements For Cryptographic Modules<br>March 2019<br>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<br>https://csrc.nist.gov/Projects/cryptographic-module-validation-program/fips-140-3-ig-announcements |
| FIPS 180-4 | Secure Hash Standard (SHS)<br>March 2012<br>https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf |
| FIPS 186-4 | Digital Signature Standard (DSS)<br>July 2013<br>https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf |
| FIPS 197 | Advanced Encryption Standard<br>November 2001<br>https://csrc.nist.gov/publications/fips/fips197/fips-197.pdf |
| FIPS 198-1 | The Keyed Hash Message Authentication Code (HMAC)<br>July 2008<br>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<br>August 2015<br>https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf |
| PKCS#1 | Public Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1<br>February 2003<br>https://www.ietf.org/rfc/rfc3447.txt |
| SP 800-38A | Recommendation for Block Cipher Modes of Operation Methods and Techniques<br>December 2001<br>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<br>October 2010<br>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<br>May 2005<br>https://csrc.nist.gov/publications/nistpubs/800-38B/SP_800-38B.pdf |


© 2026 Cloudlinux Inc., TuxCare division / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

| | |
|---|---|
| SP 800-38C | Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality<br>May 2004<br>https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38c.pdf |
| SP 800-38D | Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC<br>November 2007<br>https://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf |
| SP 800-38E | Recommendation for Block Cipher Modes of Operation: The XTS AES Mode for Confidentiality on Storage Devices<br>January 2010<br>https://csrc.nist.gov/publications/nistpubs/800-38E/nist-sp-800-38E.pdf |
| SP 800-90Ar1 | Recommendation for Random Number Generation Using Deterministic Random Bit Generators<br>June 2015<br>https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90Ar1.pdf |
| RFC 4106 | The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)<br>June 2005<br>https://datatracker.ietf.org/doc/html/rfc4106 |


© 2026 Cloudlinux Inc., TuxCare division / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.