



**Ctrl IQ, Inc.**

# **Rocky Linux 8 Kernel Cryptographic API FIPS 140-3 Non-Proprietary Security Policy**

**Prepared by:**

atsec information security corporation  
4516 Seton Center Pkwy, Suite 250  
Austin, TX 78759  
[www.atsec.com](http://www.atsec.com)

**Document version: 1.2**  
**Last update: 2025-11-12**

# 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 .....                            | 12 |
| 2.7   | Algorithm Specific Information.....                                | 15 |
| 2.7.1 | AES-GCM IV .....                                                   | 15 |
| 2.7.2 | AES-XTS.....                                                       | 15 |
| 2.7.3 | RSA.....                                                           | 16 |
| 2.7.4 | Authenticated Encryption/Decryption.....                           | 16 |
| 2.7.5 | SHA-1 .....                                                        | 16 |
| 2.8   | RBG and Entropy .....                                              | 16 |
| 2.9   | Key Generation .....                                               | 17 |
| 2.10  | Key Establishment .....                                            | 17 |
| 2.11  | Industry Protocols .....                                           | 17 |
| 3     | Cryptographic Module Interfaces .....                              | 18 |
| 3.1   | Ports and Interfaces .....                                         | 18 |
| 4     | Roles, Services, and Authentication.....                           | 19 |
| 4.1   | Authentication Methods .....                                       | 19 |
| 4.2   | Roles.....                                                         | 19 |
| 4.3   | Approved Services .....                                            | 19 |
| 4.4   | Non-Approved Services.....                                         | 23 |
| 4.5   | External Software/Firmware Loaded .....                            | 23 |
| 5     | Software/Firmware Security .....                                   | 24 |
| 5.1   | Integrity Techniques .....                                         | 24 |
| 5.2   | Initiate on Demand .....                                           | 24 |
| 6     | Operational Environment .....                                      | 25 |
| 6.1   | Operational Environment Type and Requirements.....                 | 25 |
| 6.2   | Configuration Settings and Restrictions .....                      | 25 |
| 7     | Physical Security .....                                            | 26 |

|      |                                                            |    |
|------|------------------------------------------------------------|----|
| 8    | Non-Invasive Security .....                                | 27 |
| 9    | Sensitive Security Parameters Management .....             | 28 |
| 9.1  | Storage Areas .....                                        | 28 |
| 9.2  | SSP Input-Output Methods .....                             | 28 |
| 9.3  | SSP Zeroization Methods .....                              | 28 |
| 9.4  | SSPs .....                                                 | 29 |
| 9.5  | Transitions .....                                          | 32 |
| 10   | Self-Tests .....                                           | 33 |
| 10.1 | Pre-Operational Self-Tests .....                           | 33 |
| 10.2 | Conditional Self-Tests .....                               | 33 |
| 10.3 | Periodic Self-Test Information .....                       | 40 |
| 10.4 | Error States .....                                         | 44 |
| 10.5 | Operator Initiation of Self-Tests .....                    | 45 |
| 11   | Life-Cycle Assurance .....                                 | 46 |
| 11.1 | Installation, Initialization, and Startup Procedures ..... | 46 |
| 11.2 | Administrator Guidance .....                               | 46 |
| 11.3 | Non-Administrator Guidance .....                           | 46 |
| 11.4 | Design and Rules .....                                     | 46 |
| 11.5 | Maintenance Requirements .....                             | 46 |
| 11.6 | End of Life .....                                          | 46 |
| 12   | Mitigation of Other Attacks .....                          | 48 |
| A    | Glossary and Abbreviations .....                           | 49 |
| B    | References .....                                           | 50 |

## 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 .....                                                    | 8  |
| Table 5: Approved Algorithms.....                                                            | 11 |
| Table 6: Non-Approved, Not Allowed Algorithms .....                                          | 12 |
| Table 7: Security Function Implementations .....                                             | 15 |
| Table 8: Entropy Certificates.....                                                           | 16 |
| Table 9: Entropy Sources .....                                                               | 16 |
| Table 10: Ports and Interfaces .....                                                         | 18 |
| Table 11: Roles.....                                                                         | 19 |
| Table 12: Approved Services .....                                                            | 23 |
| Table 13: Non-Approved Services .....                                                        | 23 |
| Table 14: Storage Areas.....                                                                 | 28 |
| Table 15: SSP Input-Output Methods .....                                                     | 28 |
| Table 16: SSP Zeroization Methods.....                                                       | 29 |
| Table 17: SSP Table 1.....                                                                   | 30 |
| Table 18: SSP Table 2.....                                                                   | 31 |
| Table 19: Pre-Operational Self-Tests.....                                                    | 33 |
| Table 20: Conditional Self-Tests.....                                                        | 40 |
| Table 21: Pre-Operational Periodic Information .....                                         | 40 |
| Table 22: Conditional Periodic Information .....                                             | 44 |
| Table 23: Error States .....                                                                 | 45 |

## List of Figures

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

# 1 General

## 1.1 Overview

This document is the non-proprietary FIPS 140-3 Security Policy for version kernel rocky8.20240923; libkcapi 1.2.0-2.el8 of the Rocky Linux 8 Kernel Cryptographic API module. It contains the security rules under which the module must operate and describes how this module meets the requirements as specified in FIPS PUB 140-3 (Federal Information Processing Standards Publication 140-3) for an overall Security Level 1 module.

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

### 1.1.1 How this Security Policy was prepared

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

## 1.2 Security Levels

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

Table 1: Security Levels

## 2 Cryptographic Module Specification

### 2.1 Description

**Purpose and Use:**

The Rocky Linux 8 Kernel Cryptographic API (hereafter referred to as “the module”) provides a C language application program interface (API) for use by other (kernel space and user space) processes that require cryptographic functionality. The module operates on a general-purpose computer as part of the Linux kernel. Its cryptographic functionality can be accessed using the Linux Kernel Crypto API.

**Module Type:** Software

**Module Embodiment:** MultiChipStand

**Cryptographic Boundary:**

The cryptographic boundary of the module is defined as the kernel binary and the kernel crypto object files, the libkcapi shared 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 provided by the processor is located within the module’s physical perimeter and outside of the module’s cryptographic boundary.

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

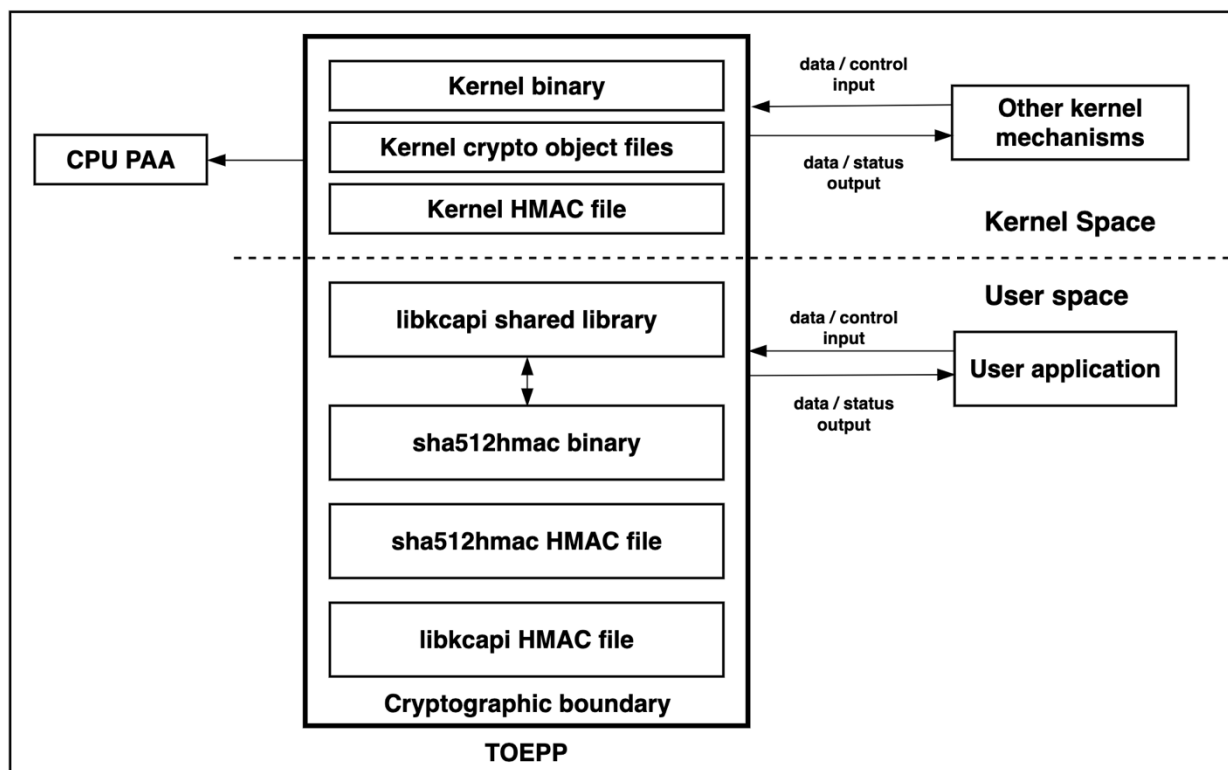


Figure 1: Block Diagram

## 2.2 Tested and Vendor Affirmed Module Version and Identification

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

| Package or File Name                                                                                                                                                                                                                                                                 | Software/<br>Firmware<br>Version             | Features | Integrity<br>Test                                                                                            |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------|----------|--------------------------------------------------------------------------------------------------------------|
| /boot/vmlinuz-4.18.0-553.16.1.el8_6.ciqfips.0.5.x86_64; *.ko.xz files in /usr/lib/modules/4.18.0-553.16.1.el8_6.ciqfips.0.5.x86_64/kernel/crypto and /usr/lib/modules/4.18.0-553.16.1.el8_6.ciqfips.0.5.x86_64/kernel/arch/x86/crypto; /usr/bin/sha512hmac; /lib64/libkcapi.so.1.2.0 | kernel rocky8.20240923; libkcapi 1.2.0-2.el8 | N/A      | HMAC-SHA2-256 (libkcapi.so); HMAC-SHA2-512 (vmlinuz, sha512hmac); RSA signature verification (*.ko.xz files) |

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

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

| Operating System | Hardware Platform             | Processors            | PAA/PAI | Hypervisor or Host OS | Version(s)                                   |
|------------------|-------------------------------|-----------------------|---------|-----------------------|----------------------------------------------|
| Rocky Linux 8    | SuperMicro SuperServer 5039MS | Intel Xeon E3-1270 v6 | Yes     |                       | kernel rocky8.20240923; libkcapi 1.2.0-2.el8 |
| Rocky Linux 8    | SuperMicro SuperServer 5039MS | Intel Xeon E3-1270 v6 | No      |                       | kernel rocky8.20240923; libkcapi 1.2.0-2.el8 |

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

The module implements Processor Algorithm Acceleration (PAA) for the tested platforms listed above. There is no Processor Algorithm Implementation (PAI).

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

N/A for this module.

## 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     | Mapped to approved service indicator in Section 4.3 for all approved algorithms except GCM: respective approved service function returns indicator 0. For GCM: <code>crypto_aead_get_flags(tfm)</code> has the <code>CRYPTO_TFM_FIPS_COMPLIANCE</code> flag set |
| Non-approved mode | Automatically entered whenever a non-approved service is requested | Non-Approved | No service indicator required for non-approved services per IG 2.4.C                                                                                                                                                                                            |

Table 4: Modes List and Description

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

### Mode Change Instructions and Status:

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

## 2.5 Algorithms

### Approved Algorithms:

| Algorithm   | CAVP Cert                                                                                               | Properties                                                                                                           | Reference  |
|-------------|---------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------|------------|
| AES-CBC     | A5807, A5810, A5813, A5816, A5819                                                                       | Direction - Decrypt, Encrypt<br>Key Length - 128, 192, 256                                                           | SP 800-38A |
| AES-CBC-CS3 | A5807, A5810, A5816, A5819                                                                              | Direction - decrypt, encrypt<br>Key Length - 128, 192, 256                                                           | SP 800-38A |
| AES-CCM     | A5807, A5810, A5816, A5819                                                                              | Key Length - 128, 192, 256                                                                                           | SP 800-38C |
| AES-CFB128  | A5807, A5810, A5816, A5819                                                                              | Direction - Decrypt, Encrypt<br>Key Length - 128, 192, 256                                                           | SP 800-38A |
| AES-CMAC    | A5807, A5810, A5816, A5819                                                                              | Direction - Generation, Verification<br>Key Length - 128, 192, 256                                                   | SP 800-38B |
| AES-CTR     | A5807, A5810, A5813, A5816, A5819                                                                       | Direction - Decrypt, Encrypt<br>Key Length - 128, 192, 256                                                           | SP 800-38A |
| AES-ECB     | A5807, A5808, A5809, A5810, A5811, A5812, A5813, A5814, A5815, A5816, A5817, A5818, A5819, A5820, A5821 | Direction - Decrypt, Encrypt<br>Key Length - 128, 192, 256                                                           | SP 800-38A |
| AES-GCM     | A5807, A5809, A5810, A5812, A5813, A5815, A5816, A5818, A5819, A5821                                    | Direction - Decrypt, Encrypt<br>IV Generation - External<br>Key Length - 128, 192, 256                               | SP 800-38D |
| AES-GCM     | A5808, A5811, A5814, A5817, A5820                                                                       | Direction - Decrypt, Encrypt<br>IV Generation - Internal<br>IV Generation Mode - 8.2.1<br>Key Length - 128, 192, 256 | SP 800-38D |
| AES-GMAC    | A5807, A5810, A5816, A5819                                                                              | Direction - Decrypt, Encrypt<br>IV Generation - External<br>Key Length - 128, 192, 256                               | SP 800-38D |
| AES-KW      | A5807, A5810, A5816, A5819                                                                              | Direction - Decrypt, Encrypt                                                                                         | SP 800-38F |

| Algorithm                          | CAVP Cert                                                                                               | Properties                                                                                               | Reference         |
|------------------------------------|---------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|-------------------|
|                                    |                                                                                                         | Key Length - 128, 192, 256                                                                               |                   |
| AES-XTS<br>Testing<br>Revision 2.0 | A5807, A5810, A5813, A5816, A5819                                                                       | Direction - Decrypt, Encrypt<br>Key Length - 128, 256                                                    | SP 800-38E        |
| Counter DRBG                       | A5807, A5808, A5809, A5810, A5811, A5812, A5813, A5814, A5815, A5816, A5817, A5818, A5819, A5820, A5821 | Prediction Resistance - No, Yes<br>Mode - AES-128, AES-192, AES-256<br>Derivation Function Enabled - Yes | SP 800-90A Rev. 1 |
| Hash DRBG                          | A5807, A5822, A5823, A5824                                                                              | Prediction Resistance - No, Yes<br>Mode - SHA-1, SHA2-256, SHA2-512                                      | SP 800-90A Rev. 1 |
| HMAC DRBG                          | A5807, A5822, A5823, A5824                                                                              | Prediction Resistance - No, Yes<br>Mode - SHA-1, SHA2-256, SHA2-512                                      | SP 800-90A Rev. 1 |
| HMAC-SHA-1                         | A5807, A5822, A5823, A5824                                                                              | Key Length - Key Length: 112-524288 Increment 8                                                          | FIPS 198-1        |
| HMAC-SHA2-224                      | A5807, A5822, A5823, A5824                                                                              | Key Length - Key Length: 112-524288 Increment 8                                                          | FIPS 198-1        |
| HMAC-SHA2-256                      | A5807, A5822, A5823, A5824                                                                              | Key Length - Key Length: 112-524288 Increment 8                                                          | FIPS 198-1        |
| HMAC-SHA2-384                      | A5807, A5822, A5823, A5824                                                                              | Key Length - Key Length: 112-524288 Increment 8                                                          | FIPS 198-1        |
| HMAC-SHA2-512                      | A5807, A5822, A5823, A5824                                                                              | Key Length - Key Length: 112-524288 Increment 8                                                          | FIPS 198-1        |
| HMAC-SHA3-224                      | A5807                                                                                                   | Key Length - Key Length: 112-524288 Increment 8                                                          | FIPS 198-1        |
| HMAC-SHA3-256                      | A5807                                                                                                   | Key Length - Key Length: 112-524288 Increment 8                                                          | FIPS 198-1        |
| HMAC-SHA3-384                      | A5807                                                                                                   | Key Length - Key Length: 112-524288 Increment 8                                                          | FIPS 198-1        |
| HMAC-SHA3-512                      | A5807                                                                                                   | Key Length - Key Length: 112-524288 Increment 8                                                          | FIPS 198-1        |
| RSA SigVer (FIPS186-5)             | A5807                                                                                                   | Modulo - 2048, 3072, 4096<br>Signature Type - pkcs1v1.5                                                  | FIPS 186-5        |
| SHA-1                              | A5807, A5822, A5823, A5824                                                                              | Message Length - Message Length: 0-                                                                      | FIPS 180-4        |

| Algorithm | CAVP Cert                  | Properties                                                                                   | Reference  |
|-----------|----------------------------|----------------------------------------------------------------------------------------------|------------|
|           |                            | 65536 Increment 8<br>Large Message Sizes -<br>1, 2                                           |            |
| SHA2-224  | A5807, A5822, A5823, A5824 | Message Length -<br>Message Length: 0-<br>65536 Increment 8<br>Large Message Sizes -<br>1, 2 | FIPS 180-4 |
| SHA2-256  | A5807, A5822, A5823, A5824 | Message Length -<br>Message Length: 0-<br>65536 Increment 8<br>Large Message Sizes -<br>1, 2 | FIPS 180-4 |
| SHA2-384  | A5807, A5822, A5823, A5824 | Message Length -<br>Message Length: 0-<br>65536 Increment 8<br>Large Message Sizes -<br>1, 2 | FIPS 180-4 |
| SHA2-512  | A5807, A5822, A5823, A5824 | Message Length -<br>Message Length: 0-<br>65536 Increment 8<br>Large Message Sizes -<br>1, 2 | FIPS 180-4 |
| SHA3-224  | A5807                      | Message Length -<br>Message Length: 0-<br>65536 Increment 8<br>Large Message Sizes -<br>1, 2 | FIPS 202   |
| SHA3-256  | A5807                      | Message Length -<br>Message Length: 0-<br>65536 Increment 8<br>Large Message Sizes -<br>1, 2 | FIPS 202   |
| SHA3-384  | A5807                      | Message Length -<br>Message Length: 0-<br>65536 Increment 8<br>Large Message Sizes -<br>1, 2 | FIPS 202   |
| SHA3-512  | A5807                      | Message Length -<br>Message Length: 0-<br>65536 Increment 8<br>Large Message Sizes -<br>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 with external IV (not compliant to FIPS 140-3 IG C.H)                                        |
| KBKDF in libkcapi                       | Key derivation with implementation not tested by CAVP                                                   |
| HKDF in libkcapi                        | Key derivation with implementation not tested by CAVP                                                   |
| PBKDF2 in libkcapi                      | Password-based key derivation with implementation not tested by CAVP                                    |
| RSA PKCS#1 v1.5 with pre-hashed message | Signature generation; Signature verification                                                            |
| RSA PKCS#1 v1.5                         | Key encapsulation (not compliant to SP 800-56Br2); Key un-encapsulation (not compliant to SP 800-56Br2) |
| RSA primitive                           | Encryption primitive; Decryption primitive (not compliant to SP 800-56Br2)                              |

Table 6: Non-Approved, Not Allowed Algorithms

**2.6 Security Function Implementations**

| Name       | Type      | Description       | Properties | Algorithms                                                                                                                                                                                                                                                                                                                                                                       |
|------------|-----------|-------------------|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Encryption | BC-UnAuth | Encrypt plaintext | a          | AES-CBC:<br>(A5807, A5810, A5813, A5816, A5819)<br>AES-CBC-CS3:<br>(A5807, A5810, A5816, A5819)<br>AES-CFB128:<br>(A5807, A5810, A5816, A5819)<br>AES-CTR:<br>(A5807, A5810, A5813, A5816, A5819)<br>AES-ECB:<br>(A5807, A5808, A5809, A5810, A5811, A5812, A5813, A5814, A5815, A5816, A5817, A5818, A5819, A5820, A5821)<br>AES-XTS Testing<br>Revision 2.0:<br>(A5807, A5810, |

| Name                     | Type      | Description                           | Properties | Algorithms                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------------------|-----------|---------------------------------------|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                          |           |                                       |            | A5813, A5816, A5819)                                                                                                                                                                                                                                                                                                                                                                               |
| Decryption               | BC-UnAuth | Decrypt a ciphertext                  |            | AES-CBC:<br>(A5807, A5810, A5813, A5816, A5819)<br>AES-CBC-CS3:<br>(A5807, A5810, A5816, A5819)<br>AES-CFB128:<br>(A5807, A5810, A5816, A5819)<br>AES-CTR:<br>(A5807, A5810, A5813, A5816, A5819)<br>AES-ECB:<br>(A5807, A5808, A5809, A5810, A5811, A5812, A5813, A5814, A5815, A5816, A5817, A5818, A5819, A5820, A5821)<br>AES-XTS Testing Revision 2.0:<br>(A5807, A5810, A5813, A5816, A5819) |
| Authenticated encryption | BC-Auth   | Encrypt and authenticate a plaintext  |            | AES-CCM:<br>(A5807, A5810, A5816, A5819)<br>AES-KW:<br>(A5807, A5810, A5816, A5819)<br>AES-GCM:<br>(A5808, A5811, A5814, A5817, A5820)                                                                                                                                                                                                                                                             |
| Authenticated decryption | BC-UnAuth | Decrypt and authenticate a ciphertext |            | AES-CCM:<br>(A5807, A5810, A5816, A5819)<br>AES-KW:<br>(A5807, A5810, A5816, A5819)<br>AES-GCM:<br>(A5807, A5809, A5810, A5812, A5813, A5815, A5816, A5818, A5819, A5821)                                                                                                                                                                                                                          |

| Name                   | Type | Description              | Properties | Algorithms                                                                                                                                                                                                                                                                                                                                                                                 |
|------------------------|------|--------------------------|------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Message digest         | SHA  | Compute a message digest |            | SHA-1: (A5807, A5822, A5823, A5824)<br>SHA2-224: (A5807, A5822, A5823, A5824)<br>SHA2-256: (A5807, A5822, A5823, A5824)<br>SHA2-384: (A5807, A5822, A5823, A5824)<br>SHA2-512: (A5807, A5822, A5823, A5824)<br>SHA3-224: (A5807)<br>SHA3-256: (A5807)<br>SHA3-384: (A5807)<br>SHA3-512: (A5807)                                                                                            |
| Message authentication | MAC  | Compute a MAC tag        |            | AES-CMAC: (A5807, A5810, A5816, A5819)<br>AES-GMAC: (A5807, A5810, A5816, A5819)<br>HMAC-SHA-1: (A5807, A5822, A5823, A5824)<br>HMAC-SHA2-224: (A5807, A5822, A5823, A5824)<br>HMAC-SHA2-256: (A5807, A5822, A5823, A5824)<br>HMAC-SHA2-384: (A5807, A5822, A5823, A5824)<br>HMAC-SHA2-512: (A5807, A5822, A5823, A5824)<br>HMAC-SHA3-224: (A5807)<br>HMAC-SHA3-256: (A5807)<br>HMAC-SHA3- |

| Name                     | Type          | Description                | Properties | Algorithms                                                                                                                                                                                                    |
|--------------------------|---------------|----------------------------|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                          |               |                            |            | 384: (A5807)<br>HMAC-SHA3-512: (A5807)                                                                                                                                                                        |
| Random number generation | DRBG          | Generate random bytes      |            | Counter DRBG: (A5807, A5808, A5809, A5810, A5811, A5812, A5813, A5814, A5815, A5816, A5817, A5818, A5819, A5820, A5821)<br>Hash DRBG: (A5807, A5822, A5823, A5824)<br>HMAC DRBG: (A5807, A5822, A5823, A5824) |
| Signature verification   | DigSig-SigVer | Verify a digital signature |            | RSA SigVer (FIPS186-5): (A5807)                                                                                                                                                                               |

Table 7: Security Function Implementations

## 2.7 Algorithm Specific Information

### 2.7.1 AES-GCM IV

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

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

The design of the IPsec protocol implicitly ensures that the counter (the nonce\_explicit part of the IV) does not exhaust the maximum number of possible values for a given session key. In the event the module's power is lost and restored, the consuming application must ensure that a new key for use with the AES-GCM key encryption or decryption under this scenario shall be established.

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

### 2.7.2 AES-XTS

The length of a single data unit encrypted or decrypted with AES-XTS shall not exceed 220 AES blocks, that is 16MB, of data per XTS instance. An XTS instance is defined in Section 4 of SP 800-38E.

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.

To meet the requirement stated in IG C.I, the module implements a check to ensure that the two AES keys used in AES XTS mode are not identical. As the module does not implement symmetric key generation, this check is performed when the keys are input by the operator. Key\_1 and Key\_2 shall be generated and/or established independently according to the rules for component symmetric keys from NIST SP 800-133r2, Section 6.3.

### 2.7.3 RSA

All supported modulus sizes for RSA signature verification have been CAVP tested.

### 2.7.4 Authenticated Encryption/Decryption

The module does not establish SSPs 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.

### 2.7.5 SHA-1

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

## 2.8 RBG and Entropy

| Cert Number | Vendor Name   |
|-------------|---------------|
| E205        | Ctrl IQ, Inc. |

Table 8: Entropy Certificates

| Name                                                           | Type         | Operational Environment                                 | Sample Size | Entropy per Sample | Conditioning Component |
|----------------------------------------------------------------|--------------|---------------------------------------------------------|-------------|--------------------|------------------------|
| Rocky Linux<br>Kernel CPU Time<br>Jitter RNG<br>Entropy Source | Non-Physical | Rocky Linux 8 on Intel<br>Kaby Lake Xeon E3-<br>1270 v6 | 256 bits    | 256 bits           | SHA3-256<br>(A5807)    |

Table 9: Entropy Sources

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

Additionally, the module employs a specific HMAC-SHA2-512 DRBG implementation for internal purposes (e.g. to generate initialization vectors). This DRBG is initially seeded with 384 output bits from the entropy source (384 bits of entropy) and reseeded with 256 output

© 2025 Ctrl IQ, Inc., atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

bits from the entropy source (256 bits of entropy). Outputs of multiple `GetEntropy()` calls are concatenated to receive the entropy input length greater than 256 bits. The output is truncated to get the entropy input string which is not a multiple of 256.

E.g. The 384 bits of entropy source output is obtained by calling the `GetEntropy()` twice, with each call providing 256 bits of output. The second call output is truncated to 128 bits and concatenated to the 256 bit output from the first call.

The module complies with the Public Use Document for ESV certificate E205 by reading entropy data from the `jent_kcapi_random()` function, which corresponds to the `GetEntropy()` conceptual interface. The operational environment on the ESV certificate is identical to the operating system described in this document. There are no maintenance requirements for the entropy source.

## **2.9 Key Generation**

The module does not implement any key generation methods.

## **2.10 Key Establishment**

The module does not implement any automated key establishment methods.

## **2.11 Industry Protocols**

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

## 3 Cryptographic Module Interfaces

### 3.1 Ports and Interfaces

| Physical Port | Logical Interface(s) | Data That Passes                                                                |
|---------------|----------------------|---------------------------------------------------------------------------------|
| N/A           | Data Input           | API data input parameters, AF_ALG type sockets                                  |
| N/A           | Data Output          | API data output parameters, AF_ALG type sockets, /proc/sys/crypto virtual files |
| N/A           | Control Input        | API function calls, API control input parameters, AF_ALG type sockets           |
| 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. These logical interfaces are logically separated from each other by the API design and AF\_ALG type socket message types.

The module does not support a control output interface.

## 4 Roles, Services, and Authentication

### 4.1 Authentication Methods

The module does not implement any authentication methods.

### 4.2 Roles

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

Table 11: Roles

No support is provided for multiple concurrent operators.

### 4.3 Approved Services

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

| Name                     | Description              | Indicator                      | Inputs                       | Outputs      | Security Functions       | SSP Access                                                                                                                                                                                                                                                                     |
|--------------------------|--------------------------|--------------------------------|------------------------------|--------------|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Message digest           | Compute a message digest | crypto_shash_init returns 0    | Message                      | Digest value | Message digest           | Crypto Officer                                                                                                                                                                                                                                                                 |
| Message authentication   | Compute a MAC tag        | crypto_shash_init returns 0    | AES key or HMAC key, message | MAC tag      | Message authentication   | Crypto Officer<br>- AES key: W,E<br>- HMAC key: W,E                                                                                                                                                                                                                            |
| Random number generation | Generate random bytes    | crypto_rng_get_bytes returns 0 | Output length                | Random bytes | Random number generation | Crypto Officer<br>- Entropy input (IG D.L): G,E,Z<br>- CTR_DRBG seed (IG D.L): G,E,Z<br>- HMAC_DRBG seed (IG D.L): G,E,Z<br>- Hash_DRBG seed (IG D.L): G,E,Z<br>- CTR_DRBG internal state (V, Key) (IG D.L): G,W,E<br>- HMAC_DRBG internal state (V, Key) (IG D.L): G,W,E<br>- |

| Name                       | Description                                                                        | Indicator | Inputs                              | Outputs                          | Security Functions                                                   | SSP Access                                                         |
|----------------------------|------------------------------------------------------------------------------------|-----------|-------------------------------------|----------------------------------|----------------------------------------------------------------------|--------------------------------------------------------------------|
|                            |                                                                                    |           |                                     |                                  |                                                                      | Hash_D<br>RBG<br>internal<br>state (V,<br>C) (IG<br>D.L):<br>G,W,E |
| Error<br>detection<br>code | Compute<br>an EDC<br>(crc32,<br>crc32c,<br>crct10dif<br>)                          | None      | Message                             | EDC                              | None                                                                 | Crypto<br>Officer                                                  |
| Compression                | Compress<br>data<br>(deflate,<br>lz4,<br>lz4hc,<br>lzo, zlib-<br>deflate,<br>zstd) | None      | Data                                | Compressed<br>data               | None                                                                 | Crypto<br>Officer                                                  |
| Generic<br>system<br>call  | Use the<br>kernel to<br>perform<br>various<br>non-<br>cryptographic<br>operations  | None      | Identifier,<br>various<br>arguments | Various<br>return<br>values      | None                                                                 | Crypto<br>Officer                                                  |
| Show<br>version            | Return<br>the<br>module<br>name<br>and<br>version<br>information                   | None      | N/A                                 | Module<br>name<br>and<br>version | None                                                                 | Crypto<br>Officer                                                  |
| Show<br>status             | Return<br>the<br>module<br>status                                                  | None      | N/A                                 | Module<br>status                 | None                                                                 | Crypto<br>Officer                                                  |
| Self-test                  | Perform<br>the<br>CASTs<br>and<br>integrity<br>tests                               | None      | N/A                                 | Pass/fail                        | Encryption<br>Decryption<br>Authenticated<br>encryption<br>Authentic | Crypto<br>Officer                                                  |

| Name        | Description  | Indicator | Inputs  | Outputs | Security Functions                                                                                                | SSP Access                                                                                                                                                                                                                                              |
|-------------|--------------|-----------|---------|---------|-------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|             |              |           |         |         | ated decryption<br>Message digest<br>Message authentication<br>Random number generation<br>Signature verification |                                                                                                                                                                                                                                                         |
| Zeroization | Zeroize SSPs | None      | Any SSP | N/A     | None                                                                                                              | Crypto Officer<br>- AES key: Z<br>- HMAC key: Z<br>- Entropy input (IG D.L): Z<br>- CTR_DRBG seed (IG D.L): Z<br>- HMAC_DRBG seed (IG D.L): Z<br>- Hash_DRBG seed (IG D.L): Z<br>- CTR_DRBG internal state (V, Key) (IG D.L): Z<br>- HMAC_DRBG internal |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access                                                                            |
|------|-------------|-----------|--------|---------|--------------------|---------------------------------------------------------------------------------------|
|      |             |           |        |         |                    | state (V, Key) (IG D.L): Z<br>-<br>Hash_D<br>RBG<br>internal state (V, C) (IG D.L): Z |

Table 12: Approved Services

For the above table, the convention below applies when specifying the access permissions (types) that the service has for each SSP.

- **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       | Encrypt and authenticate a plaintext using AES-GCM with an external IV | AES-GCM with external IV                                    | Crypto Officer |
| Key derivation                            | Derive a key from a key-derivation key, shared secret, or password     | KBKDF in libkcapi<br>HKDF in libkcapi<br>PBKDF2 in libkcapi | Crypto Officer |
| Pre-hashed message signature generation   | Generate a digital signature for a pre-hashed message                  | RSA PKCS#1 v1.5 with pre-hashed message                     | Crypto Officer |
| Pre-hashed message signature verification | Verify a digital signature for a pre-hashed message                    | RSA PKCS#1 v1.5 with pre-hashed message                     | Crypto Officer |
| Key encapsulation                         | Key encapsulation using RSA PKCS#1 v1.5                                | RSA PKCS#1 v1.5                                             | Crypto Officer |
| Key un-encapsulation                      | Key un-encapsulation using RSA PKCS#1 v1.5                             | RSA PKCS#1 v1.5                                             | Crypto Officer |
| Encryption primitive                      | Compute the RSA encryption primitive                                   | RSA primitive                                               | Crypto Officer |
| Decryption primitive                      | Compute the RSA decryption primitive                                   | RSA primitive                                               | Crypto Officer |

Table 13: Non-Approved Services

#### 4.5 External Software/Firmware Loaded

The module does not load external software or firmware.

## 5 Software/Firmware Security

### 5.1 Integrity Techniques

On system boot, the sha512hmac binary and libkcap library are first integrity tested using the HMAC-SHA2-512 and HMAC-SHA2-256 algorithms (respectively) implemented by the module. Then, the kernel binary is integrity tested using the HMAC-SHA2-512 algorithm. These tests are all performed using a key hardcoded in the sha512hmac binary, by recomputing the MAC tags and verifying they are equal to the MAC tags specified in the .hmac file.

Finally, the kernel crypto object files are loaded on start-up by the kernel binary and verified using RSA signature verification with PKCS#1 v1.5 padding, SHA2-256, and a hardcoded 3072-bit key. The signature is stored inside the kernel object file. If the signature verification fails, the integrity test is unsuccessful.

### 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 (i.e., rebooting the system), which will perform (among others) the software integrity tests.

## 6 Operational Environment

### 6.1 Operational Environment Type and Requirements

**Type of Operational Environment:** Modifiable

**How Requirements are Satisfied:**

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

### 6.2 Configuration Settings and Restrictions

The module shall be installed as stated in Section 11.1.

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

## 7 Physical Security

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

## 8 Non-Invasive Security

The module does not implement any non-invasive security mechanisms.

## 9 Sensitive Security Parameters Management

### 9.1 Storage Areas

| Storage Area Name | Description                                                                | Persistence Type |
|-------------------|----------------------------------------------------------------------------|------------------|
| Module 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; SSPs in use by the module exist in volatile memory only. 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) | Module RAM | Plaintext   | Manual            | Electronic |                  |
| AF_ALG type sockets  | Operator calling application (TOEPP) | Module RAM | Plaintext   | Manual            | Electronic |                  |

Table 15: SSP Input-Output Methods

### 9.3 SSP Zeroization Methods

| Zeroization Method           | Description                                          | Rationale                                                                                                                                                                                     | Operator Initiation                                                                                                                                                                                                                                                                                                                                      |
|------------------------------|------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Free cipher handle           | Zeroizes the SSPs contained within the cipher handle | Memory occupied by SSPs is overwritten with zeroes, which renders the SSP values irretrievable. The completion of the zeroization routine indicates that the zeroization procedure succeeded. | By calling the appropriate zeroization functions: AES key: <code>crypto_free_skcipher</code> and <code>crypto_free_aead</code> ; HMAC key: <code>crypto_free_shash</code> and <code>crypto_free_ahash</code> ; Entropy input: <code>crypto_free_rng</code> ; DRBG seed: <code>crypto_free_rng</code> ; DRBG internal state: <code>crypto_free_rng</code> |
| Remove power from the module | De-allocates the volatile memory used to store SSPs  | Volatile memory used by the module is overwritten within nanoseconds when power is removed. Module power off indicates that the                                                               | By removing power                                                                                                                                                                                                                                                                                                                                        |

| Zeroization Method | Description                                                | Rationale                                                                                       | Operator Initiation |
|--------------------|------------------------------------------------------------|-------------------------------------------------------------------------------------------------|---------------------|
|                    |                                                            | zeroization procedure succeeded.                                                                |                     |
| 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                 |

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                | Symmetric key used for AES operations                   | 128, 256 bits (AES-XTS);<br>128, 192, 256 bits (others)<br>- 128, 256 bits (AES-XTS);<br>128, 192, 256 bits (others) | Symmetric key - CSP      |                          |                | Encryption<br>Decryption<br>Message authentication<br>Authenticated encryption<br>Authenticated decryption |
| HMAC key               | Symmetric key used for HMAC operations                  | 112-524288 bits - 112-256 bits                                                                                       | Authentication key - CSP |                          |                | Message authentication                                                                                     |
| Entropy input (IG D.L) | Entropy input used to seed DRBGs (IG D.L)               | 128-384 bits - 128-384 bits                                                                                          | Entropy input - CSP      | Random number generation |                | Random number generation                                                                                   |
| CTR_DRBG seed (IG D.L) | CTR_DRBG seed derived from entropy input and additional | 256, 320, 384 bits - 128, 192, 256 bits                                                                              | Seed - CSP               | Random number generation |                | Random number generation                                                                                   |

| Name                                       | Description                                                            | Size - Strength                         | Type Category        | Generated By             | Established By | Used By                  |
|--------------------------------------------|------------------------------------------------------------------------|-----------------------------------------|----------------------|--------------------------|----------------|--------------------------|
|                                            | data (IG D.L)                                                          |                                         |                      |                          |                |                          |
| Hash_DRBG seed (IG D.L)                    | Hash_DRBG seed derived from entropy input and additional data (IG D.L) | 440, 888 bits - 128, 256 bits           | Seed - CSP           | Random number generation |                | Random number generation |
| HMAC_DRBG seed (IG D.L)                    | HMAC_DRBG seed derived from entropy input and additional data (IG D.L) | 440, 888 bits - 128, 256 bits           | Seed - CSP           | Random number generation |                | Random number generation |
| CTR_DRBG internal state (V, Key) (IG D.L)  | Internal state of CTR_DRBG (IG D.L)                                    | 256, 320, 348 bits - 128, 192, 256 bits | Internal state - CSP | Random number generation |                | Random number generation |
| HMAC_DRBG internal state (V, Key) (IG D.L) | Internal state of HMAC_DRBG (IG D.L)                                   | 320, 512, 1024 bits - 128, 256 bits     | Internal state - CSP | Random number generation |                | Random number generation |
| Hash_DRBG internal state (V, C) (IG D.L)   | Internal state of Hash_DRBG (IG D.L)                                   | 880, 1776 bits - 128, 256 bits          | Internal state - CSP | Random number generation |                | Random number generation |

Table 17: SSP Table 1

| Name     | Input - Output                           | Storage              | Storage Duration                                      | Zeroization                                     | Related SSPs |
|----------|------------------------------------------|----------------------|-------------------------------------------------------|-------------------------------------------------|--------------|
| AES key  | API input parameters AF_ALG type sockets | Module RAM:Plaintext | Until cipher handle is freed or module is powered off | Free cipher handle Remove power from the module |              |
| HMAC key | API input parameters AF_ALG              | Module RAM:Plaintext | Until cipher handle is freed or                       | Free cipher handle Remove                       |              |

| Name                                       | Input - Output | Storage              | Storage Duration                                      | Zeroization                                        | Related SSPs                                                                                         |
|--------------------------------------------|----------------|----------------------|-------------------------------------------------------|----------------------------------------------------|------------------------------------------------------------------------------------------------------|
|                                            | type sockets   |                      | module is powered off                                 | power from the module                              |                                                                                                      |
| Entropy input (IG D.L)                     |                | Module RAM:Plaintext | From generation until DRBG seed is created            | Automatic                                          | CTR_DRBG seed (IG D.L):Derives<br>HMAC_DRBG seed (IG D.L):Derives<br>Hash_DRBG seed (IG D.L):Derives |
| CTR_DRBG seed (IG D.L)                     |                | Module RAM:Plaintext | While the DRBG is being instantiated                  | Automatic                                          | Entropy input (IG D.L):Derived From<br>CTR_DRBG internal state (V, Key) (IG D.L):Derives             |
| Hash_DRBG seed (IG D.L)                    |                | Module RAM:Plaintext | While the DRBG is being instantiated                  | Automatic                                          | Entropy input (IG D.L):Derived From<br>Hash_DRBG internal state (V, C) (IG D.L):Derives              |
| HMAC_DRBG seed (IG D.L)                    |                | Module RAM:Plaintext | While the DRBG is being instantiated                  | Automatic                                          | Entropy input (IG D.L):Derived From<br>HMAC_DRBG internal state (V, Key) (IG D.L):Derives            |
| CTR_DRBG internal state (V, Key) (IG D.L)  |                | Module RAM:Plaintext | Until cipher handle is freed or module is powered off | Free cipher handle<br>Remove power from the module | CTR_DRBG seed (IG D.L):Derived From                                                                  |
| HMAC_DRBG internal state (V, Key) (IG D.L) |                | Module RAM:Plaintext | Until cipher handle is freed or module is powered off | Free cipher handle<br>Remove power from the module | HMAC_DRBG seed (IG D.L):Derived From                                                                 |
| Hash_DRBG internal state (V, C) (IG D.L)   |                | Module RAM:Plaintext | Until cipher handle is freed or module is powered off | Free cipher handle<br>Remove power from the module | Hash_DRBG seed (IG D.L):Derived From                                                                 |

Table 18: SSP Table 2

## 9.5 Transitions

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

## 10 Self-Tests

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 does not return control to the calling application until the tests are completed. If any of the self-tests fails, the module immediately transitions to the error state.

### 10.1 Pre-Operational Self-Tests

| Algorithm or Test                         | Test Properties            | Test Method            | Test Type       | Indicator                                                     | Details                                    |
|-------------------------------------------|----------------------------|------------------------|-----------------|---------------------------------------------------------------|--------------------------------------------|
| HMAC-SHA2-512 (A5824) - sha512hmac binary | 128-bit key                | Message authentication | SW/FW Integrity | Module becomes operational and services are available for use | Integrity test for sha512hmac binary       |
| HMAC-SHA2-256 (A5824) - libkcapi library  | 256-bit key                | Message authentication | SW/FW Integrity | Module becomes operational and services are available for use | Integrity test for libkcapi shared library |
| HMAC-SHA2-512 (A5824) - Kernel            | 128-bit key                | Message authentication | SW/FW Integrity | Module becomes operational and services are available for use | Integrity test for Kernel binary           |
| RSA SigVer (FIPS186-5) (A5807)            | 3072-bit key with SHA2-256 | Signature verification | SW/FW Integrity | Module becomes operational and services are available for use | Integrity test for kernel object files     |

Table 19: Pre-Operational Self-Tests

The pre-operational software integrity tests are performed automatically when the module is powered on, before the module transitions into the operational state.

### 10.2 Conditional Self-Tests

| Algorithm or Test         | Test Properties        | Test Method | Test Type | Indicator          | Details       | Conditions            |
|---------------------------|------------------------|-------------|-----------|--------------------|---------------|-----------------------|
| AES-CBC - Encrypt         | 128, 192, 256-bit keys | KAT         | CAS T     | Module operational | is Encryption | Module initialization |
| AES-CBC (A5813) - Encrypt | 128, 192, 256-bit keys | KAT         | CAS T     | Module operational | is Encryption | Module initialization |

| Algorithm or Test             | Test Properties        | Test Method | Test Type | Indicator          | Details       | Conditions            |
|-------------------------------|------------------------|-------------|-----------|--------------------|---------------|-----------------------|
| AES-CBC (A5816) - Encrypt     | 128, 192, 256-bit keys | KAT         | CAS T     | Module operational | is Encryption | Module initialization |
| AES-CBC-CS3 - Encrypt         | 128-bit keys           | KAT         | CAS T     | Module operational | is Encryption | Module initialization |
| AES-CBC-CS3 (A5816) - Encrypt | 128-bit keys           | KAT         | CAS T     | Module operational | is Encryption | Module initialization |
| AES-CCM - Encrypt             | 128, 192, 256-bit keys | KAT         | CAS T     | Module operational | is Encryption | Module initialization |
| AES-CCM (A5816) - Encrypt     | 128, 192, 256-bit keys | KAT         | CAS T     | Module operational | is Encryption | Module initialization |
| AES-CFB128 - Encrypt          | 128, 192, 256-bit keys | KAT         | CAS T     | Module operational | is Encryption | Module initialization |
| AES-CFB128 (A5816) - Encrypt  | 128, 192, 256-bit keys | KAT         | CAS T     | Module operational | is Encryption | Module initialization |
| AES-CTR - Encrypt             | 128, 192, 256-bit keys | KAT         | CAS T     | Module operational | is Encryption | Module initialization |
| AES-CTR (A5813) - Encrypt     | 128, 192, 256-bit keys | KAT         | CAS T     | Module operational | is Encryption | Module initialization |
| AES-CTR (A5816) - Encrypt     | 128, 192, 256-bit keys | KAT         | CAS T     | Module operational | is Encryption | Module initialization |
| AES-CTR (A5819) - Encrypt     | 128, 192, 256-bit keys | KAT         | CAS T     | Module operational | is Encryption | Module initialization |
| AES-ECB - Encrypt             | 128, 192, 256-bit keys | KAT         | CAS T     | Module operational | is Encryption | Module initialization |
| AES-ECB (A5810) - Encrypt     | 128, 192, 256-bit keys | KAT         | CAS T     | Module operational | is Encryption | Module initialization |
| AES-ECB (A5813) - Encrypt     | 128, 192, 256-bit keys | KAT         | CAS T     | Module operational | is Encryption | Module initialization |
| AES-ECB (A5819) - Encrypt     | 128, 192, 256-bit keys | KAT         | CAS T     | Module operational | is Encryption | Module initialization |
| AES-GCM - Encrypt             | 128, 192, 256-bit keys | KAT         | CAS T     | Module operational | is Encryption | Module initialization |

| Algorithm or Test                              | Test Properties        | Test Method | Test Type | Indicator          | Details       | Conditions            |
|------------------------------------------------|------------------------|-------------|-----------|--------------------|---------------|-----------------------|
| AES-GCM (A5815) - Encrypt                      | 128, 192, 256-bit keys | KAT         | CAS T     | Module operational | is Encryption | Module initialization |
| AES-GCM (A5818) - Encrypt                      | 128, 192, 256-bit keys | KAT         | CAS T     | Module operational | is Encryption | Module initialization |
| AES-XTS Testing Revision 2.0 - Encrypt         | 256, 512-bit keys      | KAT         | CAS T     | Module operational | is Encryption | Module initialization |
| AES-XTS Testing Revision 2.0 (A5813) - Encrypt | 256, 512-bit keys      | KAT         | CAS T     | Module operational | is Encryption | Module initialization |
| AES-CBC - Decrypt                              | 128, 192, 256-bit keys | KAT         | CAS T     | Module operational | is Decryption | Module initialization |
| AES-CBC (A5813) - Decrypt                      | 128, 192, 256-bit keys | KAT         | CAS T     | Module operational | is Decryption | Module initialization |
| AES-CBC (A5816) - Decrypt                      | 128, 192, 256-bit keys | KAT         | CAS T     | Module operational | is Decryption | Module initialization |
| AES-CBC-CS3 - Decrypt                          | 128-bit keys           | KAT         | CAS T     | Module operational | is Decryption | Module initialization |
| AES-CBC-CS3 (A5816) - Decrypt                  | 128-bit keys           | KAT         | CAS T     | Module operational | is Decryption | Module initialization |
| AES-CCM - Decrypt                              | 128, 192, 256-bit keys | KAT         | CAS T     | Module operational | is Decryption | Module initialization |
| AES-CCM (A5816) - Decrypt                      | 128, 192, 256-bit keys | KAT         | CAS T     | Module operational | is Decryption | Module initialization |
| AES-CFB128 - Decrypt                           | 128, 192, 256-bit keys | KAT         | CAS T     | Module operational | is Decryption | Module initialization |
| AES-CFB128 (A5816) - Decrypt                   | 128, 192, 256-bit keys | KAT         | CAS T     | Module operational | is Decryption | Module initialization |
| AES-CTR - Decrypt                              | 128, 192, 256-bit keys | KAT         | CAS T     | Module operational | is Decryption | Module initialization |

| Algorithm or Test                              | Test Properties        | Test Method | Test Type | Indicator          |    | Details        | Conditions            |
|------------------------------------------------|------------------------|-------------|-----------|--------------------|----|----------------|-----------------------|
| AES-CTR (A5813) - Decrypt                      | 128, 192, 256-bit keys | KAT         | CAS T     | Module operational | is | Decryption     | Module initialization |
| AES-CTR (A5816) - Decrypt                      | 128, 192, 256-bit keys | KAT         | CAS T     | Module operational | is | Decryption     | Module initialization |
| AES-CTR (A5819) - Decrypt                      | 128, 192, 256-bit keys | KAT         | CAS T     | Module operational | is | Decryption     | Module initialization |
| AES-ECB - Decrypt                              | 128, 192, 256-bit keys | KAT         | CAS T     | Module operational | is | Decryption     | Module initialization |
| AES-ECB (A5810) - Decrypt                      | 128, 192, 256-bit keys | KAT         | CAS T     | Module operational | is | Decryption     | Module initialization |
| AES-ECB (A5813) - Decrypt                      | 128, 192, 256-bit keys | KAT         | CAS T     | Module operational | is | Decryption     | Module initialization |
| AES-ECB (A5819) - Decrypt                      | 128, 192, 256-bit keys | KAT         | CAS T     | Module operational | is | Decryption     | Module initialization |
| AES-GCM - Decrypt                              | 128, 192, 256-bit keys | KAT         | CAS T     | Module operational | is | Decryption     | Module initialization |
| AES-GCM (A5815) - Decrypt                      | 128, 192, 256-bit keys | KAT         | CAS T     | Module operational | is | Decryption     | Module initialization |
| AES-GCM (A5818) - Decrypt                      | 128, 192, 256-bit keys | KAT         | CAS T     | Module operational | is | Decryption     | Module initialization |
| AES-XTS Testing Revision 2.0 - Decrypt         | 256, 512-bit keys      | KAT         | CAS T     | Module operational | is | Decryption     | Module initialization |
| AES-XTS Testing Revision 2.0 (A5813) - Decrypt | 256, 512-bit keys      | KAT         | CAS T     | Module operational | is | Decryption     | Module initialization |
| SHA-1 (A5807)                                  | 0-8184-bit messages    | KAT         | CAS T     | Module operational | is | Message digest | Module initialization |
| SHA-1 (A5822)                                  | 0-8184-bit messages    | KAT         | CAS T     | Module operational | is | Message digest | Module initialization |
| SHA-1 (A5823)                                  | 0-8184-bit messages    | KAT         | CAS T     | Module operational | is | Message digest | Module initialization |

| Algorithm or Test | Test Properties     | Test Method | Test Type | Indicator          |    | Details        | Conditions            |
|-------------------|---------------------|-------------|-----------|--------------------|----|----------------|-----------------------|
| SHA-1 (A5824)     | 0-8184-bit messages | KAT         | CAS T     | Module operational | is | Message digest | Module initialization |
| SHA2-224 (A5807)  | 0-8184-bit messages | KAT         | CAS T     | Module operational | is | Message digest | Module initialization |
| SHA2-224 (A5822)  | 0-8184-bit messages | KAT         | CAS T     | Module operational | is | Message digest | Module initialization |
| SHA2-224 (A5823)  | 0-8184-bit messages | KAT         | CAS T     | Module operational | is | Message digest | Module initialization |
| SHA2-224 (A5824)  | 0-8184-bit messages | KAT         | CAS T     | Module operational | is | Message digest | Module initialization |
| SHA2-256 (A5807)  | 0-8184-bit messages | KAT         | CAS T     | Module operational | is | Message digest | Module initialization |
| SHA2-256 (A5822)  | 0-8184-bit messages | KAT         | CAS T     | Module operational | is | Message digest | Module initialization |
| SHA2-256 (A5823)  | 0-8184-bit messages | KAT         | CAS T     | Module operational | is | Message digest | Module initialization |
| SHA2-256 (A5824)  | 0-8184-bit messages | KAT         | CAS T     | Module operational | is | Message digest | Module initialization |
| SHA2-384 (A5807)  | 0-8184-bit messages | KAT         | CAS T     | Module operational | is | Message digest | Module initialization |
| SHA2-384 (A5822)  | 0-8184-bit messages | KAT         | CAS T     | Module operational | is | Message digest | Module initialization |
| SHA2-384 (A5823)  | 0-8184-bit messages | KAT         | CAS T     | Module operational | is | Message digest | Module initialization |
| SHA2-384 (A5824)  | 0-8184-bit messages | KAT         | CAS T     | Module operational | is | Message digest | Module initialization |
| SHA2-512 (A5807)  | 0-8184-bit messages | KAT         | CAS T     | Module operational | is | Message digest | Module initialization |
| SHA2-512 (A5822)  | 0-8184-bit messages | KAT         | CAS T     | Module operational | is | Message digest | Module initialization |
| SHA2-512 (A5823)  | 0-8184-bit messages | KAT         | CAS T     | Module operational | is | Message digest | Module initialization |

| Algorithm or Test     | Test Properties     | Test Method | Test Type | Indicator          |    | Details                | Conditions            |
|-----------------------|---------------------|-------------|-----------|--------------------|----|------------------------|-----------------------|
| SHA2-512 (A5824)      | 0-8184-bit messages | KAT         | CAS T     | Module operational | is | Message digest         | Module initialization |
| SHA3-224 (A5807)      | 0-8184-bit messages | KAT         | CAS T     | Module operational | is | Message digest         | Module initialization |
| SHA3-256 (A5807)      | 0-8184-bit messages | KAT         | CAS T     | Module operational | is | Message digest         | Module initialization |
| SHA3-384 (A5807)      | 0-8184-bit messages | KAT         | CAS T     | Module operational | is | Message digest         | Module initialization |
| SHA3-512 (A5807)      | 0-8184-bit messages | KAT         | CAS T     | Module operational | is | Message digest         | Module initialization |
| AES-CMAC              | 128, 256-bit keys   | KAT         | CAS T     | Module operational | is | Message authentication | Module initialization |
| AES-CMAC (A5816)      | 128, 256-bit keys   | KAT         | CAS T     | Module operational | is | Message authentication | Module initialization |
| HMAC-SHA-1            | 32-64-bit keys      | KAT         | CAS T     | Module operational | is | Message authentication | Module initialization |
| HMAC-SHA-1 (A5824)    | 32-64-bit keys      | KAT         | CAS T     | Module operational | is | Message authentication | Module initialization |
| HMAC-SHA2-224         | 32-1048-bit keys    | KAT         | CAS T     | Module operational | is | Message authentication | Module initialization |
| HMAC-SHA2-224 (A5824) | 32-1048-bit keys    | KAT         | CAS T     | Module operational | is | Message authentication | Module initialization |
| HMAC-SHA2-256         | 32-64-bit keys      | KAT         | CAS T     | Module operational | is | Message authentication | Module initialization |
| HMAC-SHA2-256 (A5824) | 32-64-bit keys      | KAT         | CAS T     | Module operational | is | Message authentication | Module initialization |
| HMAC-SHA2-384         | 32-1048-bit keys    | KAT         | CAS T     | Module operational | is | Message authentication | Module initialization |
| HMAC-SHA2-384 (A5824) | 32-1048-bit keys    | KAT         | CAS T     | Module operational | is | Message authentication | Module initialization |
| HMAC-SHA2-512         | 32-1048-bit keys    | KAT         | CAS T     | Module operational | is | Message authentication | Module initialization |

| Algorithm or Test                 | Test Properties                                              | Test Method | Test Type | Indicator                     | Details                                                                         | Conditions                    |
|-----------------------------------|--------------------------------------------------------------|-------------|-----------|-------------------------------|---------------------------------------------------------------------------------|-------------------------------|
| HMAC-SHA2-512 (A5824)             | 32-1048-bit keys                                             | KAT         | CAS T     | Module operational            | is Message authentication                                                       | Module initialization         |
| HMAC-SHA3-224 (A5807)             | 32-1048-bit keys                                             | KAT         | CAS T     | Module operational            | is Message authentication                                                       | Module initialization         |
| HMAC-SHA3-256 (A5807)             | 32-1048-bit keys                                             | KAT         | CAS T     | Module operational            | is Message authentication                                                       | Module initialization         |
| HMAC-SHA3-384 (A5807)             | 32-1048-bit keys                                             | KAT         | CAS T     | Module operational            | is Message authentication                                                       | Module initialization         |
| HMAC-SHA3-512 (A5807)             | 32-1048-bit keys                                             | KAT         | CAS T     | Module operational            | is Message authentication                                                       | Module initialization         |
| Counter DRBG                      | AES-128, AES-192, AES-256 with/without prediction resistance | KAT         | CAS T     | Module operational            | is Instantiate, seed, reseed, generate (compliant to SP 800-90Ar1 Section 11.3) | Module initialization         |
| Hash DRBG                         | SHA-1, SHA2-256, SHA2-512 with/without prediction resistance | KAT         | CAS T     | Module operational            | is Instantiate, seed, reseed, generate (compliant to SP 800-90Ar1 Section 11.3) | Module initialization         |
| HMAC DRBG                         | SHA-1, SHA2-256, SHA2-512 with/without prediction resistance | KAT         | CAS T     | Module operational            | is Instantiate, seed, reseed, generate (compliant to SP 800-90Ar1 Section 11.3) | Module initialization         |
| RSA SigVer (FIPS186-5) (A5807)    | PKCS#1 v1.5 with SHA-512 and 4096-bit key                    | KAT         | CAS T     | Module operational            | is Signature verification                                                       | Module initialization         |
| Entropy source APT initialization | Cutoff C = 325; Windows size = 512                           | APT         | CAS T     | Entropy source is operational | Entropy source start-up test on 1024 samples                                    | Entropy source initialization |
| Entropy source RCT initialization | Cutoff C = 31                                                | RCT         | CAS T     | Entropy source is operational | Entropy source start-up test on 1024 samples                                    | Entropy source initialization |

© 2025 Ctrl IQ, Inc., atsec information security.

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                           |
|-------------------------------|------------------------------------|-------------|-----------|-----------------------------|--------------------------------|--------------------------------------|
| Entropy source continuous APT | Cutoff C = 355; Windows size = 512 | APT         | CAS T     | jent_kcapi_random returns 0 | Entropy source continuous test | Continuously as entropy is requested |
| Entropy source continuous RCT | Cutoff C = 61                      | RCT         | CAS T     | jent_kcapi_random returns 0 | Entropy source continuous test | Continuously as entropy is requested |

Table 20: Conditional Self-Tests

### 10.3 Periodic Self-Test Information

| Algorithm or Test                         | Test Method            | Test Type       | Period    | Periodic Method |
|-------------------------------------------|------------------------|-----------------|-----------|-----------------|
| HMAC-SHA2-512 (A5824) - sha512hmac binary | Message authentication | SW/FW Integrity | On demand | Manually        |
| HMAC-SHA2-256 (A5824) - libkcapi library  | Message authentication | SW/FW Integrity | On demand | Manually        |
| HMAC-SHA2-512 (A5824) - Kernel            | Message authentication | SW/FW Integrity | On demand | Manually        |
| RSA SigVer (FIPS186-5) (A5807)            | Signature verification | SW/FW Integrity | On demand | Manually        |

Table 21: Pre-Operational Periodic Information

| Algorithm or Test           | Test Method | Test Type | Period    | Periodic Method |
|-----------------------------|-------------|-----------|-----------|-----------------|
| AES-CBC Encrypt             | KAT         | CAST      | On demand | Manually        |
| AES-CBC (A5813) Encrypt     | KAT         | CAST      | On demand | Manually        |
| AES-CBC (A5816) Encrypt     | KAT         | CAST      | On demand | Manually        |
| AES-CBC-CS3 Encrypt         | KAT         | CAST      | On demand | Manually        |
| AES-CBC-CS3 (A5816) Encrypt | KAT         | CAST      | On demand | Manually        |
| AES-CCM Encrypt             | KAT         | CAST      | On demand | Manually        |

| <b>Algorithm or Test</b>                       | <b>Test Method</b> | <b>Test Type</b> | <b>Period</b> | <b>Periodic Method</b> |
|------------------------------------------------|--------------------|------------------|---------------|------------------------|
| AES-CCM (A5816) Encrypt -                      | KAT                | CAST             | On demand     | Manually               |
| AES-CFB128 Encrypt -                           | KAT                | CAST             | On demand     | Manually               |
| AES-CFB128 (A5816) Encrypt -                   | KAT                | CAST             | On demand     | Manually               |
| AES-CTR Encrypt -                              | KAT                | CAST             | On demand     | Manually               |
| AES-CTR (A5813) Encrypt -                      | KAT                | CAST             | On demand     | Manually               |
| AES-CTR (A5816) Encrypt -                      | KAT                | CAST             | On demand     | Manually               |
| AES-CTR (A5819) Encrypt -                      | KAT                | CAST             | On demand     | Manually               |
| AES-ECB Encrypt -                              | KAT                | CAST             | On demand     | Manually               |
| AES-ECB (A5810) Encrypt -                      | KAT                | CAST             | On demand     | Manually               |
| AES-ECB (A5813) Encrypt -                      | KAT                | CAST             | On demand     | Manually               |
| AES-ECB (A5819) Encrypt -                      | KAT                | CAST             | On demand     | Manually               |
| AES-GCM Encrypt -                              | KAT                | CAST             | On demand     | Manually               |
| AES-GCM (A5815) Encrypt -                      | KAT                | CAST             | On demand     | Manually               |
| AES-GCM (A5818) Encrypt -                      | KAT                | CAST             | On demand     | Manually               |
| AES-XTS Testing Revision 2.0 - Encrypt         | KAT                | CAST             | On demand     | Manually               |
| AES-XTS Testing Revision 2.0 (A5813) - Encrypt | KAT                | CAST             | On demand     | Manually               |
| AES-CBC Decrypt -                              | KAT                | CAST             | On demand     | Manually               |
| AES-CBC (A5813) Decrypt -                      | KAT                | CAST             | On demand     | Manually               |

| <b>Algorithm or Test</b>               | <b>Test Method</b> | <b>Test Type</b> | <b>Period</b> | <b>Periodic Method</b> |
|----------------------------------------|--------------------|------------------|---------------|------------------------|
| AES-CBC (A5816) Decrypt -              | KAT                | CAST             | On demand     | Manually               |
| AES-CBC-CS3 Decrypt -                  | KAT                | CAST             | On demand     | Manually               |
| AES-CBC-CS3 (A5816) Decrypt -          | KAT                | CAST             | On demand     | Manually               |
| AES-CCM Decrypt -                      | KAT                | CAST             | On demand     | Manually               |
| AES-CCM (A5816) Decrypt -              | KAT                | CAST             | On demand     | Manually               |
| AES-CFB128 Decrypt -                   | KAT                | CAST             | On demand     | Manually               |
| AES-CFB128 (A5816) Decrypt -           | KAT                | CAST             | On demand     | Manually               |
| AES-CTR Decrypt -                      | KAT                | CAST             | On demand     | Manually               |
| AES-CTR (A5813) Decrypt -              | KAT                | CAST             | On demand     | Manually               |
| AES-CTR (A5816) Decrypt -              | KAT                | CAST             | On demand     | Manually               |
| AES-CTR (A5819) Decrypt -              | KAT                | CAST             | On demand     | Manually               |
| AES-ECB Decrypt -                      | KAT                | CAST             | On demand     | Manually               |
| AES-ECB (A5810) Decrypt -              | KAT                | CAST             | On demand     | Manually               |
| AES-ECB (A5813) Decrypt -              | KAT                | CAST             | On demand     | Manually               |
| AES-ECB (A5819) Decrypt -              | KAT                | CAST             | On demand     | Manually               |
| AES-GCM Decrypt -                      | KAT                | CAST             | On demand     | Manually               |
| AES-GCM (A5815) Decrypt -              | KAT                | CAST             | On demand     | Manually               |
| AES-GCM (A5818) Decrypt -              | KAT                | CAST             | On demand     | Manually               |
| AES-XTS Testing Revision 2.0 Decrypt - | KAT                | CAST             | On demand     | Manually               |

| <b>Algorithm or Test</b>                              | <b>Test Method</b> | <b>Test Type</b> | <b>Period</b> | <b>Periodic Method</b> |
|-------------------------------------------------------|--------------------|------------------|---------------|------------------------|
| AES-XTS Testing<br>Revision 2.0<br>(A5813)<br>Decrypt | KAT                | CAST             | On demand     | Manually               |
| SHA-1 (A5807)                                         | KAT                | CAST             | On demand     | Manually               |
| SHA-1 (A5822)                                         | KAT                | CAST             | On demand     | Manually               |
| SHA-1 (A5823)                                         | KAT                | CAST             | On demand     | Manually               |
| SHA-1 (A5824)                                         | KAT                | CAST             | On demand     | Manually               |
| SHA2-224<br>(A5807)                                   | KAT                | CAST             | On demand     | Manually               |
| SHA2-224<br>(A5822)                                   | KAT                | CAST             | On demand     | Manually               |
| SHA2-224<br>(A5823)                                   | KAT                | CAST             | On demand     | Manually               |
| SHA2-224<br>(A5824)                                   | KAT                | CAST             | On demand     | Manually               |
| SHA2-256<br>(A5807)                                   | KAT                | CAST             | On demand     | Manually               |
| SHA2-256<br>(A5822)                                   | KAT                | CAST             | On demand     | Manually               |
| SHA2-256<br>(A5823)                                   | KAT                | CAST             | On demand     | Manually               |
| SHA2-256<br>(A5824)                                   | KAT                | CAST             | On demand     | Manually               |
| SHA2-384<br>(A5807)                                   | KAT                | CAST             | On demand     | Manually               |
| SHA2-384<br>(A5822)                                   | KAT                | CAST             | On demand     | Manually               |
| SHA2-384<br>(A5823)                                   | KAT                | CAST             | On demand     | Manually               |
| SHA2-384<br>(A5824)                                   | KAT                | CAST             | On demand     | Manually               |
| SHA2-512<br>(A5807)                                   | KAT                | CAST             | On demand     | Manually               |
| SHA2-512<br>(A5822)                                   | KAT                | CAST             | On demand     | Manually               |
| SHA2-512<br>(A5823)                                   | KAT                | CAST             | On demand     | Manually               |
| SHA2-512<br>(A5824)                                   | KAT                | CAST             | On demand     | Manually               |
| SHA3-224<br>(A5807)                                   | KAT                | CAST             | On demand     | Manually               |
| SHA3-256<br>(A5807)                                   | KAT                | CAST             | On demand     | Manually               |
| SHA3-384<br>(A5807)                                   | KAT                | CAST             | On demand     | Manually               |
| SHA3-512<br>(A5807)                                   | KAT                | CAST             | On demand     | Manually               |
| AES-CMAC                                              | KAT                | CAST             | On demand     | Manually               |
| AES-CMAC<br>(A5816)                                   | KAT                | CAST             | On demand     | Manually               |

| Algorithm or Test                 | Test Method | Test Type | Period    | Periodic Method |
|-----------------------------------|-------------|-----------|-----------|-----------------|
| HMAC-SHA-1                        | KAT         | CAST      | On demand | Manually        |
| HMAC-SHA-1 (A5824)                | KAT         | CAST      | On demand | Manually        |
| HMAC-SHA2-224                     | KAT         | CAST      | On demand | Manually        |
| HMAC-SHA2-224 (A5824)             | KAT         | CAST      | On demand | Manually        |
| HMAC-SHA2-256                     | KAT         | CAST      | On demand | Manually        |
| HMAC-SHA2-256 (A5824)             | KAT         | CAST      | On demand | Manually        |
| HMAC-SHA2-384                     | KAT         | CAST      | On demand | Manually        |
| HMAC-SHA2-384 (A5824)             | KAT         | CAST      | On demand | Manually        |
| HMAC-SHA2-512                     | KAT         | CAST      | On demand | Manually        |
| HMAC-SHA2-512 (A5824)             | KAT         | CAST      | On demand | Manually        |
| HMAC-SHA3-224 (A5807)             | KAT         | CAST      | On demand | Manually        |
| HMAC-SHA3-256 (A5807)             | KAT         | CAST      | On demand | Manually        |
| HMAC-SHA3-384 (A5807)             | KAT         | CAST      | On demand | Manually        |
| HMAC-SHA3-512 (A5807)             | KAT         | CAST      | On demand | Manually        |
| Counter DRBG                      | KAT         | CAST      | On demand | Manually        |
| Hash DRBG                         | KAT         | CAST      | On demand | Manually        |
| HMAC DRBG                         | KAT         | CAST      | On demand | Manually        |
| RSA SigVer (FIPS186-5) (A5807)    | KAT         | CAST      | On demand | Manually        |
| Entropy source APT initialization | APT         | CAST      | On demand | Manually        |
| Entropy source RCT initialization | RCT         | CAST      | On demand | Manually        |
| Entropy source continuous APT     | APT         | CAST      | On demand | Manually        |
| Entropy source continuous RCT     | RCT         | CAST      | On demand | Manually        |

Table 22: Conditional Periodic Information

## 10.4 Error States

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

© 2025 Ctrl IQ, Inc., atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

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

All self-tests, except for the entropy source continuous health tests, can be invoked on demand by unloading and subsequently re-initializing the module.

# 11 Life-Cycle Assurance

## 11.1 Installation, Initialization, and Startup Procedures

The module is distributed as a part of the Rocky Linux 8 distribution, in the form of the kernel-4.18.0-553.16.1.el8\_6.ciqfips.0.5, libkcapi-1.2.0-2.el8, and libkcapi-hmaccalc-1.2.0-2.el8 RPM packages.

The module can achieve FIPS validated configuration by:

- Adding 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 the validated configuration after installation. Execute the “fips- mode-setup --enable” command. Restart the system.

In both cases, the Crypto Officer must verify the system operates in the validated configuration by executing the “fips-mode-setup --check” command, which should output “FIPS mode is enabled.”

## 11.2 Administrator Guidance

After installation of the 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:

*Rocky Linux 8 - Kernel Cryptographic API*

Then, the Crypto Officer must execute the “cat /proc/sys/crypto/fips\_version” and “rpm -qa | grep kcapi” commands. These commands must output the following (one line per output):

```
$ cat /proc/sys/crypto/fips_version
rocky8.20240923
```

```
$ rpm -qa | grep kcapi
libkcapi-hmaccalc-1.2.0-2.el8.x86_64
libkcapi-1.2.0-2.el8.x86_64
```

## 11.3 Non-Administrator Guidance

There is no non-administrator guidance.

## 11.4 Design and Rules

Not applicable.

## 11.5 Maintenance Requirements

Not applicable.

## 11.6 End of Life

As the module does not persistently store SSPs, secure sanitization of the module consists of unloading the module. This will zeroize all SSPs in volatile memory. Then, if desired, the kernel-4.18.0-553.16.1.el8\_6.ciqfips.0.5, libkcapi-1.2.0-2.el8, and libkcapi-hmacalc-1.2.0-2.el8 RPM packages can be uninstalled from the Rocky Linux 8 system.

## 12 Mitigation of Other Attacks

The module does not implement security mechanisms to mitigate other attacks.

## A Glossary and Abbreviations

|                |                                                                |
|----------------|----------------------------------------------------------------|
| <b>AES</b>     | Advanced Encryption Standard                                   |
| <b>API</b>     | Application Programming Interface                              |
| <b>CAST</b>    | Cryptographic Algorithm Self-Test                              |
| <b>CAVP</b>    | Cryptographic Algorithm Validation Program                     |
| <b>CBC</b>     | Cipher Block Chaining                                          |
| <b>CBC-CS3</b> | Cipher Block Chaining with Ciphertext Stealing 3               |
| <b>CCM</b>     | Counter with Cipher Block Chaining-Message Authentication Code |
| <b>CFB</b>     | Cipher Feedback                                                |
| <b>CMAC</b>    | Cipher-based Message Authentication Code                       |
| <b>CMVP</b>    | Cryptographic Module Validation Program                        |
| <b>CSP</b>     | Critical Security Parameter                                    |
| <b>CTR</b>     | Counter                                                        |
| <b>DRBG</b>    | Deterministic Random Bit Generator                             |
| <b>ECB</b>     | Electronic Code Book                                           |
| <b>FIPS</b>    | Federal Information Processing Standards                       |
| <b>GCM</b>     | Galois Counter Mode                                            |
| <b>GMAC</b>    | Galois Counter Mode Message Authentication Code                |
| <b>HMAC</b>    | Keyed-Hash Message Authentication Code                         |
| <b>IPsec</b>   | Internet Protocol Security                                     |
| <b>IG</b>      | Implementation Guidance                                        |
| <b>IV</b>      | Initialization Vector                                          |
| <b>KAT</b>     | Known Answer Test                                              |
| <b>KW</b>      | Key Wrap                                                       |
| <b>MAC</b>     | Message Authentication Code                                    |
| <b>NIST</b>    | National Institute of Science and Technology                   |
| <b>PAA</b>     | Processor Algorithm Acceleration                               |
| <b>PAI</b>     | Processor Algorithm Implementation                             |
| <b>PCT</b>     | Pair-wise Consistency Test                                     |
| <b>PSP</b>     | Public Security Parameter                                      |
| <b>RSA</b>     | Rivest Shamir Adleman                                          |
| <b>SHA</b>     | Secure Hash Algorithm                                          |
| <b>SSP</b>     | Sensitive Security Parameter                                   |
| <b>TOEPP</b>   | Tested Operational Environment's Physical Perimeter            |
| <b>XTS</b>     | XEX-based Tweaked-codebook mode with cipher text Stealing      |

## B References

- FIPS 140-3**      **Security Requirements For Cryptographic Modules**  
March 2019  
<https://doi.org/10.6028/NIST.FIPS.140-3>
- FIPS 140-3 IG**      **Implementation Guidance for FIPS PUB 140-3 and the Cryptographic Module Validation Program**  
<https://csrc.nist.gov/CSRC/media/Projects/cryptographic-module-validation-program/documents/fips%20140-3/FIPS%20140-3%20IG.pdf>
- FIPS 180-4**      **Secure Hash Standard (SHS)**  
August 2015  
<https://doi.org/10.6028/NIST.FIPS.180-4>
- FIPS 186-5**      **Digital Signature Standard (DSS)**  
February 2023  
<https://doi.org/10.6028/NIST.FIPS.186-5>
- FIPS 197**      **Advanced Encryption Standard (AES)**  
November 2001; Updated May 2023  
<https://doi.org/10.6028/NIST.FIPS.197-upd1>
- FIPS 198-1**      **The Keyed-Hash Message Authentication Code (HMAC)**  
July 2008  
<https://doi.org/10.6028/NIST.FIPS.198-1>
- FIPS 202**      **SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions**  
August 2015  
<https://doi.org/10.6028/NIST.FIPS.202>
- PKCS#1**      **PKCS #1: RSA Cryptography Specifications Version 2.2**  
November 2016  
<https://doi.org/10.17487/RFC8017>
- SP 800-38A**      **Recommendation for Block Cipher Modes of Operation: Methods and Techniques**  
December 2001  
<https://doi.org/10.6028/NIST.SP.800-38A>
- SP 800-38A-Add**      **Recommendation for Block Cipher Modes of Operation: Three Variants of Ciphertext Stealing for CBC Mode**  
October 2010  
<https://doi.org/10.6028/NIST.SP.800-38A-Add>
- SP 800-38B**      **Recommendation for Block Cipher Modes of Operation: the CMAC Mode for Authentication**  
May 2005; Updated October 2016  
<https://doi.org/10.6028/NIST.SP.800-38B>
- SP 800-38C**      **Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality**  
May 2004; Updated July 2007  
<https://doi.org/10.6028/NIST.SP.800-38C>
- SP 800-38D**      **Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC**  
November 2007  
<https://doi.org/10.6028/NIST.SP.800-38D>
- SP 800-38E**      **Recommendation for Block Cipher Modes of Operation: the XTS-AES Mode for Confidentiality on Storage Devices**  
January 2010  
<https://doi.org/10.6028/NIST.SP.800-38E>
- SP 800-38F**      **Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping**

- December 2012  
<https://doi.org/10.6028/NIST.SP.800-38F>  
**SP 800-90Ar1 Recommendation for Random Number Generation Using Deterministic Random Bit Generators**
- June 2015  
<https://doi.org/10.6028/NIST.SP.800-90Ar1>  
**SP 800-90B Recommendation for the Entropy Sources Used for Random Bit Generation**
- January 2018  
<https://doi.org/10.6028/NIST.SP.800-90B>  
**SP 800-131Ar2 Transitioning the Use of Cryptographic Algorithms and Key Lengths**
- March 2019  
<https://doi.org/10.6028/NIST.SP.800-131Ar2>  
**SP 800-140Br1 Cryptographic Module Validation Program (CMVP) Security Policy Requirements: CMVP Validation Authority Updates to ISO/IEC 24759 and ISO/IEC 19790 Annex B**
- November 2023  
<https://doi.org/10.6028/NIST.SP.800-140Br1>