Red Hat, Inc.

Red Hat Enterprise Linux 8 Kernel Cryptographic API

FIPS 140-3 Non-Proprietary Security Policy

Document Version: 1.3

Last Modified: 09/16/2024

Prepared by:

atsec information security corporation

4516 Seton Center Parkway, Suite 250

Austin, TX 78759

www.atsec.com

Table of Contents

List of Tables

List of Figures

1 General

1.1 Overview

This document is the non-proprietary FIPS 140-3 Security Policy for version kernel 4.18.0-372.52.1.el8_6; libkcapi 1.2.0-2.el8 of the Red Hat Enterprise 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

1.3 Additional Information [O]

Not applicable.

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

The Red Hat Enterprise 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: Multi-chip standalone

Module Characteristics:

Cryptographic Boundary:

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

Tested Operational Environment’s Physical Perimeter (TOEPP) [O]:

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

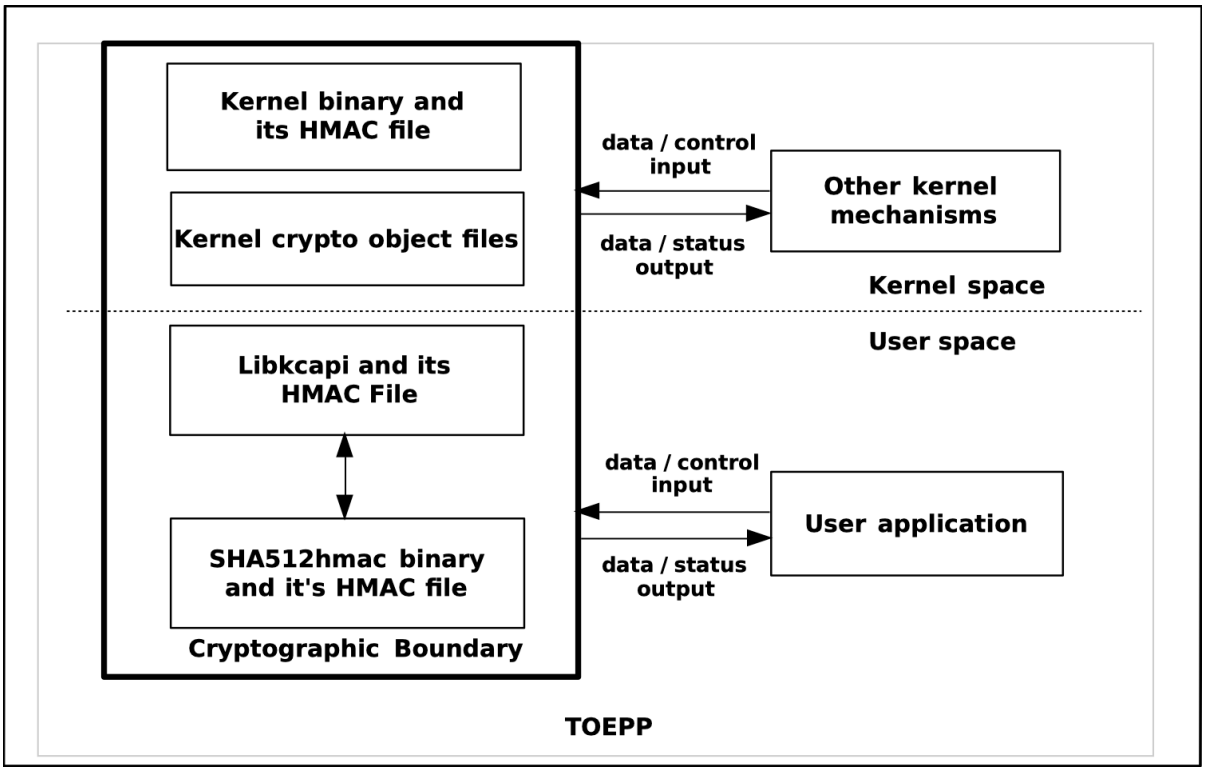

Figure 1: Block Diagram

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Hardware:

N/A for this module.

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

Package or File Name	Software/ Firmware Version	Features	Integrity Test
/boot/vmlinuz-4.18.0-372.52.1.el8_6.x86_64; *.ko and *.ko.xz files in /usr/lib/modules/4.18.0-372.52.1.el8_6.x86_64/kernel/crypto *.ko and *.ko.xz files in /usr/lib/modules/4.18.0-372.52.1.el8_6.x86_64/kernel/arch/x86/crypto; /usr/lib64/libkcapi.so.1.2.0, /usr/bin/sha512hmac	4.18.0-372.52.1.el8_6; 1.2.0-2.el8	N/A	HMAC-SHA2-512; RSA signature verification

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

Tested Module Identification – Hybrid Disjoint Hardware:

N/A for this module.

Tested Operational Environments - Software, Firmware, Hybrid:

Operating System	Hardware Platform	Processors	PAA/PAI	Hypervisor or Host OS	Version(s)
Red Hat Enterprise Linux 8	Dell PowerEdge R440	Intel Xeon Silver 4216	Yes	N/A	4.18.0-372.52.1.el8_6 1.2.0-2.el8
Red Hat Enterprise Linux 8	Dell PowerEdge R440	Intel Xeon Silver 4216	No	N/A	4.18.0-372.52.1.el8_6; 1.2.0-2.el8

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

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

Operating System	Hardware Platform
Red Hat Enterprise Linux 8	Intel Xeon E5

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

CMVP makes no statement as to the correct operation of the module or the security strengths of the generated keys when so ported if the specific operational environment is not listed on the validation certificate.

2.3 Excluded Components

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

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Type	Status Indicator
Approved mode	Automatically entered whenever an approved service is requested	Approved	Equivalent to the indicator of the requested service as defined in section 4.3
Non-approved mode	Automatically entered whenever a non-approved service is requested	Non-Approved	Equivalent to the indicator of the requested service as defined in section 4.3

Table 5: Modes List and Description

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

Mode Change Instructions and Status [O]:

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.

Degraded Mode Description [O]:

The module does not implement a degraded mode of operation.

2.5 Algorithms

Approved Algorithms:

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	A3648	-	SP 800-38A
AES-CCM	A3648	-	SP 800-38C
AES-CMAC	A3648	-	SP 800-38B
AES-CTR	A3648	-	SP 800-38A
AES-ECB	A3648	-	SP 800-38A
AES-GCM	A3648	-	SP 800-38D
AES-GMAC	A3648	-	SP 800-38D
AES-XTS Testing Revision 2.0	A3648	-	SP 800-38E
Counter DRBG	A3648	-	SP 800-90A Rev. 1
Hash DRBG	A3648	-	SP 800-90A Rev. 1
HMAC DRBG	A3648	-	SP 800-90A Rev. 1
HMAC-SHA-1	A3648	-	FIPS 198-1
HMAC-SHA2-224	A3648	-	FIPS 198-1
HMAC-SHA2-256	A3648	-	FIPS 198-1
HMAC-SHA2-384	A3648	-	FIPS 198-1
HMAC-SHA2-512	A3648	-	FIPS 198-1
RSA SigVer (FIPS186-4)	A3648	-	FIPS 186-4
SHA-1	A3648	-	FIPS 180-4
SHA2-224	A3648	-	FIPS 180-4
SHA2-256	A3648	-	FIPS 180-4
SHA2-384	A3648	-	FIPS 180-4
SHA2-512	A3648	-	FIPS 180-4
HMAC-SHA3-224	A3649	-	FIPS 198-1
HMAC-SHA3-256	A3649	-	FIPS 198-1
HMAC-SHA3-384	A3649	-	FIPS 198-1
HMAC-SHA3-512	A3649	-	FIPS 198-1
SHA3-224	A3649	-	FIPS 202
SHA3-256	A3649	-	FIPS 202
SHA3-384	A3649	-	FIPS 202
SHA3-512	A3649	-	FIPS 202
AES-CFB128	A3650	-	SP 800-38A
AES-CBC-CS3	A3651	-	SP 800-38A
AES-ECB	A3652	-	SP 800-38A
AES-GCM	A3652	-	SP 800-38D
Counter DRBG	A3652	-	SP 800-90A Rev. 1
Hash DRBG	A3652	-	SP 800-90A Rev. 1
HMAC DRBG	A3652	-	SP 800-90A Rev. 1

Algorithm	CAVP Cert	Properties	Reference
AES-ECB	A3653	-	SP 800-38A
AES-GCM	A3653	-	SP 800-38D
Counter DRBG	A3653	-	SP 800-90A Rev. 1
Hash DRBG	A3653	-	SP 800-90A Rev. 1
HMAC DRBG	A3653	-	SP 800-90A Rev. 1
AES-CBC	A3654	-	SP 800-38A
AES-CTR	A3654	-	SP 800-38A
AES-ECB	A3654	-	SP 800-38A
AES-GCM	A3654	-	SP 800-38D
AES-XTS Testing Revision 2.0	A3654	-	SP 800-38E
Counter DRBG	A3654	-	SP 800-90A Rev. 1
Hash DRBG	A3654	-	SP 800-90A Rev. 1
HMAC DRBG	A3654	-	SP 800-90A Rev. 1
AES-ECB	A3655	-	SP 800-38A
AES-GCM	A3655	-	SP 800-38D
Counter DRBG	A3655	-	SP 800-90A Rev. 1
Hash DRBG	A3655	-	SP 800-90A Rev. 1
HMAC DRBG	A3655	-	SP 800-90A Rev. 1
AES-ECB	A3656	-	SP 800-38A
AES-GCM	A3656	-	SP 800-38D
Counter DRBG	A3656	-	SP 800-90A Rev. 1
Hash DRBG	A3656	-	SP 800-90A Rev. 1
HMAC DRBG	A3656	-	SP 800-90A Rev. 1
AES-CBC	A3657	-	SP 800-38A
AES-CCM	A3657	-	SP 800-38C
AES-CMAC	A3657	-	SP 800-38B
AES-CTR	A3657	-	SP 800-38A
AES-ECB	A3657	-	SP 800-38A
AES-GCM	A3657	-	SP 800-38D
AES-GMAC	A3657	-	SP 800-38D
AES-XTS Testing Revision 2.0	A3657	-	SP 800-38E
Counter DRBG	A3657	-	SP 800-90A Rev. 1
Hash DRBG	A3657	-	SP 800-90A Rev. 1
HMAC DRBG	A3657	-	SP 800-90A Rev. 1
AES-ECB	A3658	-	SP 800-38A
AES-GCM	A3658	-	SP 800-38D
Counter DRBG	A3658	-	SP 800-90A Rev. 1
Hash DRBG	A3658	-	SP 800-90A Rev. 1
HMAC DRBG	A3658	-	SP 800-90A Rev. 1
AES-ECB	A3659	-	SP 800-38A
AES-GCM	A3659	-	SP 800-38D
Counter DRBG	A3659	-	SP 800-90A Rev. 1
Hash DRBG	A3659	-	SP 800-90A Rev. 1
HMAC DRBG	A3659	-	SP 800-90A Rev. 1
AES-CFB128	A3660	-	SP 800-38A
AES-CBC-CS3	A3661	-	SP 800-38A
Hash DRBG	A3662	-	SP 800-90A Rev. 1
HMAC DRBG	A3662	-	SP 800-90A Rev. 1
HMAC-SHA-1	A3662	-	FIPS 198-1
HMAC-SHA2-224	A3662	-	FIPS 198-1

Algorithm	CAVP Cert	Properties	Reference
HMAC-SHA2-256	A3662	-	FIPS 198-1
HMAC-SHA2-384	A3662	-	FIPS 198-1
HMAC-SHA2-512	A3662	-	FIPS 198-1
RSA SigVer (FIPS186-4)	A3662	-	FIPS 186-4
SHA-1	A3662	-	FIPS 180-4
SHA2-224	A3662	-	FIPS 180-4
SHA2-256	A3662	-	FIPS 180-4
SHA2-384	A3662	-	FIPS 180-4
SHA2-512	A3662	-	FIPS 180-4
Hash DRBG	A3663	-	SP 800-90A Rev. 1
HMAC DRBG	A3663	-	SP 800-90A Rev. 1
HMAC-SHA-1	A3663	-	FIPS 198-1
HMAC-SHA2-224	A3663	-	FIPS 198-1
HMAC-SHA2-256	A3663	-	FIPS 198-1
HMAC-SHA2-384	A3663	-	FIPS 198-1
HMAC-SHA2-512	A3663	-	FIPS 198-1
RSA SigVer (FIPS186-4)	A3663	-	FIPS 186-4
SHA-1	A3663	-	FIPS 180-4
SHA2-224	A3663	-	FIPS 180-4
SHA2-256	A3663	-	FIPS 180-4
SHA2-384	A3663	-	FIPS 180-4
SHA2-512	A3663	-	FIPS 180-4
Hash DRBG	A3664	-	SP 800-90A Rev. 1
HMAC DRBG	A3664	-	SP 800-90A Rev. 1
HMAC-SHA-1	A3664	-	FIPS 198-1
HMAC-SHA2-224	A3664	-	FIPS 198-1
HMAC-SHA2-256	A3664	-	FIPS 198-1
HMAC-SHA2-384	A3664	-	FIPS 198-1
HMAC-SHA2-512	A3664	-	FIPS 198-1
RSA SigVer (FIPS186-4)	A3664	-	FIPS 186-4
SHA-1	A3664	-	FIPS 180-4
SHA2-224	A3664	-	FIPS 180-4
SHA2-256	A3664	-	FIPS 180-4
SHA2-384	A3664	-	FIPS 180-4
SHA2-512	A3664	-	FIPS 180-4

Table 6: Approved Algorithms

Vendor-Affirmed Algorithms:

N/A for this module.

Non-Approved, Allowed Algorithms:

N/A for this module.

Non-Approved, Allowed Algorithms with No Security Claimed:

N/A for this module.

Non-Approved, Not Allowed Algorithms:

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

Table 7: Non-Approved, Not Allowed Algorithms

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
Encryption with AES	BC-UnAuth	Encrypt a plaintext with AES	Key size(s):128, 192, 256 bits (XTS mode 128 and 256 bits only)	AES-CBC AES-CBC AES-CBC AES-CBC-CS3 AES-CBC-CS3 AES-CFB128 AES-CFB128 AES-CTR AES-CTR AES-CTR AES-ECB AES-ECB AES-ECB AES-ECB AES-ECB AES-ECB AES-ECB AES-ECB AES-ECB AES-XTS Testing Revision 2.0 AES-XTS Testing Revision 2.0 AES-XTS Testing Revision 2.0
Decryption with AES	BC-UnAuth	Decrypt a ciphertext with AES	Key size(s):128, 192, 256 bits (XTS mode 128 and 256 bits only)	AES-CBC AES-CBC AES-CBC AES-CBC-CS3 AES-CBC-CS3 AES-CFB128 AES-CFB128 AES-CTR

Name	Type	Description	Properties	Algorithms
				AES-CTR AES-CTR AES-ECB AES-ECB AES-ECB AES-ECB AES-ECB AES-ECB AES-ECB AES-ECB AES-ECB AES-XTS Testing Revision 2.0 AES-XTS Testing Revision 2.0 AES-XTS Testing Revision 2.0
Hashing	SHA	Compute a message digest	SHA-1:N/A SHA2-224:N/A SHA2-256:N/A SHA2-384:N/A SHA2-512:N/A SHA3-224:N/A SHA3-256:N/A SHA3-384:N/A SHA3-512:N/A	SHA-1 SHA-1 SHA-1 SHA-1 SHA2-224 SHA2-224 SHA2-224 SHA2-224 SHA2-256 SHA2-256 SHA2-256 SHA2-256 SHA2-384 SHA2-384 SHA2-384 SHA2-384 SHA2-512 SHA2-512 SHA2-512 SHA2-512 SHA3-224 SHA3-256 SHA3-384 SHA3-512
Message authentication	MAC	Compute a MAC tag for authentication	HMAC key size(s):112-524288 bits (112-256 bits) AES key size(s):128, 192, 256 bits	AES-CMAC AES-CMAC AES-GMAC AES-GMAC HMAC-SHA-1 HMAC-SHA-1 HMAC-SHA-1 HMAC-SHA-1

Name	Type	Description	Properties	Algorithms
				HMAC-SHA2-224 HMAC-SHA2-224 HMAC-SHA2-224 HMAC-SHA2-224 HMAC-SHA2-256 HMAC-SHA2-256 HMAC-SHA2-256 HMAC-SHA2-256 HMAC-SHA2-384 HMAC-SHA2-384 HMAC-SHA2-384 HMAC-SHA2-384 HMAC-SHA2-512 HMAC-SHA2-512 HMAC-SHA2-512 HMAC-SHA2-512 HMAC-SHA3-224 HMAC-SHA3-256 HMAC-SHA3-384 HMAC-SHA3-512
Random number generation with DRBGs	DRBG	Generate random numbers from DRBGs	Counter DRBG:128, 192, 256 bits HMAC DRBG:SHA-1, SHA-256, SHA-512 Hash DRBG:SHA-1, SHA-256, SHA-512	Counter DRBG Counter DRBG Counter DRBG Counter DRBG Counter DRBG Counter DRBG Counter DRBG Counter DRBG Hash DRBG Hash DRBG Hash DRBG

Name	Type	Description	Properties	Algorithms
				Hash DRBG Hash DRBG Hash DRBG Hash DRBG Hash DRBG Hash DRBG Hash DRBG Hash DRBG Hash DRBG HMAC DRBG HMAC DRBG HMAC DRBG HMAC DRBG HMAC DRBG HMAC DRBG HMAC DRBG HMAC DRBG HMAC DRBG HMAC DRBG HMAC DRBG HMAC DRBG
Signature verification with RSA	DigSig-SigVer	Verify a signature with RSA	Padding:PKCS#1 v1.5 Hashes:SHA-256 Key size(s):3072 bits (128 bits)	RSA SigVer (FIPS186-4) RSA SigVer (FIPS186-4) RSA SigVer (FIPS186-4) RSA SigVer (FIPS186-4) RSA SigVer (FIPS186-4) RSA SigVer (FIPS186-4) RSA SigVer (FIPS186-4) RSA SigVer (FIPS186-4)
Authenticated encryption with AES	BC-Auth	Encrypt and authenticate a plaintext with AES	Key size(s):128, 192, 256 bits	AES-CCM AES-CCM AES-GCM AES-GCM AES-GCM AES-CBC AES-CBC AES-CBC AES-CTR AES-CTR AES-CTR HMAC-SHA-1 HMAC-SHA2-256 HMAC-SHA2-

Name	Type	Description	Properties	Algorithms
				384 HMAC-SHA2-512 HMAC-SHA-1 HMAC-SHA2-256 HMAC-SHA2-384 HMAC-SHA2-512 HMAC-SHA-1 HMAC-SHA2-256 HMAC-SHA2-384 HMAC-SHA2-512 HMAC-SHA-1 HMAC-SHA2-256 HMAC-SHA2-384 HMAC-SHA2-512
Authenticated decryption with AES	BC-Auth	Decrypt and authenticate a ciphertext with AES	Key size(s):128, 192, 256 bits	AES-CCM AES-CCM AES-GCM AES-GCM AES-GCM AES-GCM AES-GCM AES-GCM AES-CBC AES-CBC AES-CBC AES-CTR AES-CTR AES-CTR HMAC-SHA-1 HMAC-SHA2-256 HMAC-SHA2-384 HMAC-SHA2-512 HMAC-SHA-1 HMAC-SHA2-256 HMAC-SHA2-384 HMAC-SHA2-512

Name	Type	Description	Properties	Algorithms
				HMAC-SHA-1 HMAC-SHA2-256 HMAC-SHA2-384 HMAC-SHA2-512 HMAC-SHA-1 HMAC-SHA2-256 HMAC-SHA2-384 HMAC-SHA2-512
Key wrapping	KTS-Wrap	Key wrapping	Key size(s):128, 192, 256 bits	AES-GCM AES-GCM AES-GCM
Key unwrapping	KTS-Wrap	Key unwrapping	Key size(s):128, 192, 256 bits	AES-GCM AES-GCM AES-GCM AES-GCM AES-GCM AES-GCM

Table 8: Security Function Implementations

2.7 Algorithm Specific Information

Legacy use:
Digital Signature Verification with SHA-1 is allowed for legacy use only.

2.7.1 AES GCM IV

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

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

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

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

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

2.7.2 AES XTS

The length of a single data unit encrypted or decrypted with AES XTS shall not exceed 2^{20} AES blocks, that is 16MB, of data per XTS instance. An XTS instance is defined in Section 4 of SP 800-38E. To meet the requirement stated in IG C.I, the module implements a check to ensure that the two AES keys used in AES XTS mode are not identical.

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

2.7.3 RSA

For RSA signature verification, the module supports modulus size 3072 and 4096 bits. The supported modulus size has been CAVP tested.

2.7.4 SHA-3

The module provides SHA-3 hash functions compliant with IG C.C. Every implementation of each SHA-3 function was tested and validated on all the module's operating environments. SHAKE functions are not implemented. SHA-3 hash functions are also used as part of a higher-level algorithm for HMAC.

2.8 RBG and Entropy

Cert Number	Vendor Name
E54	Red Hat, Inc.

Table 9: Entropy Certificates

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
RHEL Kernel CPU Time Jitter RNG Entropy Source	Non-Physical	Red Hat Enterprise Linux 8 on Dell PowerEdge R440	64 bits	59.62 bits	Linear-Feedback Shift Register (LFSR)

Table 10: Entropy Sources

The module implements three different Deterministic Random Bit Generator (DRBG) implementations based on SP 800-90Ar1: Counter 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 (357 bits of entropy) and reseeded with 256 output bits from the entropy source (238 bits of entropy).

2.9 Key Generation

The module does not provide key generation.

2.10 Key Establishment

As permitted by IG D.G, the module provides key transport methods by using AES-GCM encryption mode in the context of IPsec protocol.

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.

2.12 Additional Information [O]

Not applicable.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

Physical Port	Logical Interface(s)	Data That Passes
As a software-only module, the module does not have physical ports. Physical ports are interpreted to be the physical ports of the hardware platform on which it runs.	Data Input	API data input parameters, AF_ALG type sockets
As a software-only module, the module does not have physical ports. Physical ports are interpreted to be the physical ports of the hardware platform on which it runs.	Data Output	API data output parameters, AF_ALG type sockets
As a software-only module, the module does not have physical ports. Physical ports are interpreted to be the physical ports of the hardware platform on which it runs.	Control Input	API function calls, API control input parameters, AF_ALG type sockets, kernel command line
As a software-only module, the module does not have physical ports. Physical Ports are interpreted to be the physical ports of the hardware platform on which it runs.	Status Output	API return values, AF_ALG type sockets, kernel logs

Table 11: Ports and Interfaces

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

3.2 Trusted Channel Specification [O]

The module does not implement a trusted channel.

3.3 Control Interface Not Inhibited [O]

The module does not implement a control output interface.

3.4 Additional Information [O]

Not applicable.

4 Roles, Services, and Authentication

4.1 Authentication Methods

N/A for this module.

The module does not implement authentication.

4.2 Roles

Name	Type	Operator Type	Authentication Methods
Crypto Officer	Role	CO	None

Table 12: Roles

The module supports the Crypto Officer role only. This sole role is implicitly and always assumed by the operator of the module. No support is provided for multiple concurrent operators.

4.3 Approved Services

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Message digest	Compute a message digest	crypto_shash_init returns 0	Message	Digest value	Hashing	Crypto Officer
Key wrapping	Wrap a key	crypto_skcipher_setkey returns 0; crypto_shash_init returns 0	AES key, key to be wrapped	wrapped key	Key wrapping	Crypto Officer - AES key: W,E - HMAC key: W,E
Key unwrapping	Unwrap a key	crypto_skcipher_setkey returns 0; crypto_shash_init returns 0	AES key, key to be unwrapped	unwrapped key	Key unwrapping	Crypto Officer - AES key: W,E - HMAC

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						key: W,E
Encryption	Encrypt a plaintext	crypto_skcipher_setkey returns 0	AES key, plaintext	Ciphertext	Encryption with AES	Crypto Officer - AES key: W,E
Decryption	Decrypt a ciphertext	crypto_skcipher_setkey returns 0	AES key, ciphertext	Plaintext	Decryption with AES	Crypto Officer - AES key: W,E
Authenticated encryption	Encrypt and authenticate a plaintext	For all except AES GCM: crypto_aead_setkey returns 0; For AES GCM: crypto_aead_get_flags(tfm) has the CRYPTO_TFM_FIPS_COMPLIANCE flag set	AES key, plaintext	Ciphertext, MAC tag	Authenticated encryption with AES	Crypto Officer - AES key: W,E
Authenticated decryption	Encrypt and authenticate a ciphertext	For all except AES GCM: crypto_aead_setkey returns 0; For AES GCM: crypto_aead_get_flags(tfm) has the CRYPTO_TFM_FIPS_COMPLIANCE flag set	AES key, ciphertext, MAC tag	Plaintext or failure	Authenticated decryption with AES	Crypto Officer - AES key: W,E
Message authentication generation	Compute a MAC tag	crypto_shash_init returns 0	AES: AES key, message; HMAC: HMAC key, message	MAC tag	Message authentication	Crypto Officer - AES key: W,E - HMAC key: W,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Message authentication verification	Compute a MAC tag	crypto_shash_init returns 0	AES: AES key, message, MAC tag; HMAC: HMAC key, message, MAC tag	Success/Failure	Message authentication	Crypto Officer - AES key: W,E - HMAC key: W,E
Random number generation	Generate random bytes	crypto_rng_get_bytes returns 0	Output length	Random bytes	Random number generation with DRBGs	Crypto Officer - Entropy input: W,E - DRBG seed: G,E - DRBG Internal state (V, Key): G,W,E - DRBG Internal state (V, C): G,W,E
Error detection code	Compute an EDC (crc32, crct10dif)	None	Message	EDC	None	Crypto Officer

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Compression	Compress data (deflate, lz4, lz4hc, lzo, zlibdeflate, zstd)	None	Data	Compressed data	None	Crypto Officer
Generic system call	Use the kernel to perform various non-cryptographic operations	None	Identifier, various arguments	Various return values	None	Crypto Officer
Show version	Return the module name and version information	None	N/A	Module name and version	None	Crypto Officer
Show status	Return the module status	None	N/A	Module status	None	Crypto Officer
Self-test	Perform the CASTs and integrity tests	None	N/A	Pass/fail	Encryption with AES Decryption with AES Hashing Message authentication Random number generation with DRBGs Signature verification with RSA Authenticated encryption with AES Authenticated	Crypto Officer

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					decryption with AES	
Zeroization	Zeroize all SSPs	None	Any SSP	N/A	None	Crypto Officer - AES key: Z - HMAC key: Z - Entropy input: Z - DRBG Internal state (V, Key): Z - DRBG Internal state (V, C): Z - DRBG seed: Z

Table 13: Approved Services

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

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

- **Zeroize (Z):** The module zeroizes the SSP.

4.4 Non-Approved Services

Name	Description	Algorithms	Role
AES GCM external IV encryption	Encrypt a plaintext using AES GCM with an external IV	AES-GCM with external IV	CO
Key derivation	Derive a key from a key-derivation key or a shared secret	KBKDF (libkcapi) HKDF (libkcapi)	CO
Password-based key derivation	Derive a key from a password	PBKDF2 (libkcapi)	CO
RSA encryption primitive	Compute the raw RSA encryption of a plaintext	RSA	CO
RSA decryption primitive	Compute the raw RSA decryption of a cipertext	RSA	CO
RSA signature generation (pre-hashed message)	Generate a digital signature for a pre-hashed message	RSA with PKCS#1 v1.5 padding	CO
RSA signature verification (pre-hashed message)	Verify a digital signature for a pre-hashed message	RSA with PKCS#1 v1.5 padding	CO

Table 14: Non-Approved Services

4.5 External Software/Firmware Loaded

The module does not load external software or firmware.

4.6 Bypass Actions and Status [O]

The module does not implement a bypass capability.

4.7 Cryptographic Output Actions and Status [O]

The module does not implement a self-initiated cryptographic output capability.

4.8 Additional Information [O]

Not applicable.

5 Software/Firmware Security

5.1 Integrity Techniques

The Linux kernel binary is integrity tested using an HMAC-SHA2-512 calculation performed by the sha512hmac utility (which utilizes the module's HMAC and SHA-512 implementations). An HMAC-SHA2-512 calculation is also performed on the sha512hmac utility and the libkcapi library to verify their integrity. The kernel crypto object files listed in section 2.2 are loaded on start-up by the module and verified using RSA signature verification with PKCS#1 v1.5 padding, SHA-256, and a 3072-bit key.

5.2 Initiate on Demand

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

5.3 Open-Source Parameters [O]

Not applicable.

5.4 Additional Information [O]

Not applicable.

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Modifiable

How Requirements are Satisfied [O]:

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 [O]

The module shall be installed as stated in Section 11.1.

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

6.3 Additional Information [O]

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

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

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

7 Physical Security

7.1 Mechanisms and Actions Required [O]

N/A for this module.

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

7.2 User Placed Tamper Seals [O]

Not applicable.

7.3 Filler Panels [O]

Not applicable.

7.4 Fault Induction Mitigation [O]

Not applicable.

7.5 EFP/EFT Information [O]

Temp/Voltage Type	Temperature or Voltage	EFP or EFT	Result
LowTemperature			
HighTemperature			
LowVoltage			
HighVoltage			

Table 15: EFP/EFT Information

Not applicable.

7.6 Hardness Testing Temperature Ranges [O]

Temperature Type	Temperature
LowTemperature	
HighTemperature	

Table 16: Hardness Testing Temperatures

Not applicable.

7.7 Additional Information [O]

Not applicable.

8 Non-Invasive Security

8.1 Mitigation Techniques [O]

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

8.2 Effectiveness [O]

Not applicable.

8.3 Additional Information [O]

Not applicable.

9 Sensitive Security Parameters Management

9.1 Storage Areas

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

Table 17: Storage Areas

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

9.2 SSP Input-Output Methods

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

Table 18: 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: crypto_free_skcipher and crypto_free_aead; HMAC key: crypto_free_shash and crypto_free_ahash; DRBG internal state: crypto_free_rng; DRBG seed: crypto_free_rng; Entropy input string: crypto_free_rng;
Remove power from the module	De-allocates the volatile memory used to store SSPs	Volatile memory used by the module is overwritten within nanoseconds when power is removed. Module power off indicates that the zeroization procedure succeeded. The	By removing power

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

Table 19: SSP Zeroization Methods

All data output is inhibited during zeroization.

9.4 SSPs

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
AES key	AES key used for encryption, decryption, and computing MAC tags.	128, 192, 256 bits - 128, 192, 256 bits	Symmetric Key - CSP			Encryption with AES Decryption with AES Authenticated encryption with AES Authenticated decryption with AES Key wrapping Key unwrapping
HMAC key	HMAC key.	112-524288 bits - 112-256 bits	Authentication key - CSP			Message authentication
Entropy input	Entropy input used to seed the DRBGs. Compliant with IG D.L.	128-384 bits - 117-357 bits	Entropy input - CSP			Random number generation with DRBGs
DRBG seed	DRBG seed derived from entropy input. Compliant with IG D.L.	Counter DRBG: 128, 192, 256 bits; Hash DRBG: 128, 256 bits; HMAC DRBG: 128, 256	Seed - CSP	Random number generation with DRBGs		Random number generation with DRBGs

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
		bits - Counter DRBG: 128, 192, 256 bits; Hash DRBG: 128, 256 bits; HMAC DRBG: 128, 256 bits				
DRBG Internal state (V, Key)	Internal state of Counter DRBG and HMAC DRBG instances. Compliant with IG D.L.	Counter DRBG: 128, 192, 256 bits; HMAC DRBG: 128, 256 bits - Counter DRBG: 128, 192, 256 bits; HMAC DRBG: 128, 256 bits	Internal state - CSP	Random number generation with DRBGs		Random number generation with DRBGs
DRBG Internal state (V, C)	Internal state of Hash DRBG instances. Compliant with IG D.L.	Hash DRBG: 128, 256 bits - Hash DRBG: 128, 256 bits	Internal state - CSP	Random number generation with DRBGs		Random number generation with DRBGs

Table 20: SSP Table 1

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

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

Table 21: SSP Table 2

9.5 Transitions [O]

The SHA-1 algorithm as implemented by the module will be non-approved for all purposes, starting January 1, 2030.

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

9.6 Additional Information [O]

Not applicable.

10 Self-Tests

10.1 Pre-Operational Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
HMAC-SHA2-512 (A3664)	128-bit key	Message Authentication	SW/FW Integrity	Module becomes operational and services are available for use.	Integrity test for vmlinuz, libkcapi components and sha512hmac binary
RSA SigVer (FIPS186-4) (A3648)	3072-bit key with SHA-256	Signature Verification	SW/FW Integrity	Module becomes operational and services are available for use.	Integrity test for kernel object files

Table 22: Pre-Operational Self-Tests

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

10.2 Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
SHA-1 (A3648)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA-1 (A3662)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
SHA-1 (A3663)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA-1 (A3664)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-224 (A3648)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-224 (A3662)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-224 (A3663)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-224 (A3664)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-256 (A3648)	0-8184 bit messages	KAT	CAST	Module becomes operational	Message digest	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				and services are available for use.		
SHA2-256 (A3662)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-256 (A3663)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-256 (A3664)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-384 (A3648)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-384 (A3662)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-384 (A3663)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are	Message digest	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				available for use.		
SHA2-384 (A3664)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-512 (A3648)	0-8184 bit message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-512 (A3662)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-512 (A3663)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-512 (A3664)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA3-224 (A3649)	0-8184 bit message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
SHA3-256 (A3649)	0-8184 bit message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA3-384 (A3649)	0-8184 bit message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA3-512 (A3649)	0-8184 bit message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
AES-ECB (A3648)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Encryption, Decryption	Module initialization
AES-ECB (A3652)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Encryption, Decryption	Module initialization
AES-ECB (A3653)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Encryption, Decryption	Module initialization
AES-ECB (A3654)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Encryption, Decryption	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				and services are available for use.		
AES-ECB (A3655)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Encryption, Decryption	Module initialization
AES-ECB (A3656)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Encryption, Decryption	Module initialization
AES-ECB (A3658)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Encryption, Decryption	Module initialization
AES-ECB (A3659)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Encryption, Decryption	Module initialization
AES-ECB (A3657)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Encryption, Decryption	Module initialization
AES-CBC (A3648)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are	Encryption, Decryption	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				available for use.		
AES-CBC (A3654)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Encryption, Decryption	Module initialization
AES-CBC-CS3 (A3661)	128 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Encryption, Decryption	Module initialization
AES-CFB128 (A3660)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Encryption, Decryption	Module initialization
AES-CTR (A3648)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Encryption, Decryption	Module initialization
AES-CTR (A3657)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Encryption, Decryption	Module initialization
AES-CCM (A3657)	128, 192, 256 bit keys; 128-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Encryption, Decryption	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-GCM (A3648)	128, 192, 256 bit keys, 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Encryption, Decryption	Module initialization
AES-GCM (A3652)	128, 192, 256 bit keys, 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Encryption	Module initialization
AES-GCM (A3653)	128, 192, 256 bit keys, 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Encryption, Decryption	Module initialization
AES-GCM (A3654)	128, 192, 256 bit keys, 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Encryption, Decryption	Module initialization
AES-GCM (A3655)	128, 192, 256 bit keys, 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Encryption	Module initialization
AES-GCM (A3656)	128, 192, 256 bit keys, 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Encryption, Decryption	Module initialization
AES-GCM (A3657)	128, 192, 256 bit keys, 96-bit IVs	KAT	CAST	Module becomes operational	Encryption, Decryption	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				and services are available for use.		
AES-GCM (A3658)	128, 192, 256 bit keys, 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Encryption	Module initialization
AES-GCM (A3659)	128, 192, 256 bit keys, 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Encryption, Decryption	Module initialization
AES-XTS Testing Revision 2.0 (A3648)	128 and 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Encryption, Decryption	Module initialization
AES-XTS Testing Revision 2.0 (A3657)	128 and 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Encryption, Decryption	Module initialization
AES-CMAC (A3657)	128 and 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
HMAC-SHA-1 (A3648)	32-64 bit keys	KAT	CAST	Module becomes operational and services are	Message authentication	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				available for use.		
HMAC-SHA-1 (A3662)	32-64 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
HMAC-SHA-1 (A3663)	32-64 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
HMAC-SHA-1 (A3664)	32-64 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
HMAC-SHA2-224 (A3648)	32-1048 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
HMAC-SHA2-224 (A3662)	32-1048 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
HMAC-SHA2-224 (A3663)	32-1048 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HMAC-SHA2-224 (A3664)	32-1048 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
HMAC-SHA2-256 (A3648)	32-64 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
HMAC-SHA2-256 (A3662)	32-64 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
HMAC-SHA2-256 (A3663)	32-64 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
HMAC-SHA2-256 (A3664)	32-64 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
HMAC-SHA2-384 (A3648)	32-1048 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
HMAC-SHA2-384 (A3662)	32-1048 bit keys	KAT	CAST	Module becomes operational	Message authentication	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				and services are available for use.		
HMAC-SHA2-384 (A3663)	32-1048 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
HMAC-SHA2-384 (A3664)	32-1048 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
HMAC-SHA2-512 (A3648)	32-1048 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization. Before integrity test.
HMAC-SHA2-512 (A3662)	32-1048 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization. Before integrity test.
HMAC-SHA2-512 (A3663)	32-1048 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization. Before integrity test.
HMAC-SHA2-512 (A3664)	32-1048 bit keys	KAT	CAST	Module becomes operational and services are	Message authentication	Module initialization. Before integrity test.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				available for use.		
HMAC-SHA3-224 (A3649)	32-1048 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
HMAC-SHA3-256 (A3649)	32-1048 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
HMAC-SHA3-384 (A3649)	32-1048 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
HMAC-SHA3-512 (A3649)	32-1048 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
Counter DRBG (A3648)	128, 192, 256 bit keys With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Seed, Generate	Module initialization
Counter DRBG (A3652)	128, 192, 256 bit keys With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Seed, Generate	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
Counter DRBG (A3653)	128, 192, 256 bit keys With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Seed, Generate	Module initialization
Counter DRBG (A3654)	128, 192, 256 bit keys With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Seed, Generate	Module initialization
Counter DRBG (A3655)	128, 192, 256 bit keys With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Seed, Generate	Module initialization
Counter DRBG (A3656)	128, 192, 256 bit keys With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Seed, Generate	Module initialization
Counter DRBG (A3657)	128, 192, 256 bit keys With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Seed, Generate	Module initialization
Counter DRBG (A3658)	128, 192, 256 bit keys With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Seed, Generate	Module initialization
Counter DRBG (A3659)	128, 192, 256 bit keys With/without	KAT	CAST	Module becomes operational	Seed, Generate	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
	PR; Health test per section 11.3 of SP 800-90Arev1			and services are available for use.		
Hash DRBG (A3648)	SHA-256 With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Seed, Generate	Module initialization
Hash DRBG (A3652)	SHA-256 With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Seed, Generate	Module initialization
Hash DRBG (A3653)	SHA-256 With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Seed, Generate	Module initialization
Hash DRBG (A3654)	SHA-256 With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Seed, Generate	Module initialization
Hash DRBG (A3655)	SHA-256 With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Seed, Generate	Module initialization
Hash DRBG (A3656)	SHA-256 With/without PR; Health test per section 11.3	KAT	CAST	Module becomes operational and services are	Seed, Generate	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
	of SP 800-90Arev1			available for use.		
Hash DRBG (A3657)	SHA-256 With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Seed, Generate	Module initialization
Hash DRBG (A3658)	SHA-256 With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Seed, Generate	Module initialization
Hash DRBG (A3659)	SHA-256 With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Seed, Generate	Module initialization
Hash DRBG (A3662)	SHA-256 With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Seed, Generate	Module initialization
Hash DRBG (A3663)	SHA-256 With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Seed, Generate	Module initialization
Hash DRBG (A3664)	SHA-256 With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Seed, Generate	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HMAC DRBG (A3648)	SHA-256, SHA512 With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Seed, Generate	Module initialization
HMAC DRBG (A3652)	SHA-256, SHA512 With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Seed, Generate	Module initialization
HMAC DRBG (A3653)	SHA-256, SHA512 With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Seed, Generate	Module initialization
HMAC DRBG (A3654)	SHA-256, SHA512 With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Seed, Generate	Module initialization
HMAC DRBG (A3655)	SHA-256, SHA512 With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Seed, Generate	Module initialization
HMAC DRBG (A3656)	SHA-256, SHA512 With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Seed, Generate	Module initialization
HMAC DRBG (A3657)	SHA-256, SHA512 With/without	KAT	CAST	Module becomes operational	Seed, Generate	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
	PR; Health test per section 11.3 of SP 800-90Arev1			and services are available for use.		
HMAC DRBG (A3658)	SHA-256, SHA512 With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Seed, Generate	Module initialization
HMAC DRBG (A3659)	SHA-256, SHA512 With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Seed, Generate	Module initialization
HMAC DRBG (A3662)	SHA-256, SHA512 With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Seed, Generate	Module initialization
HMAC DRBG (A3663)	SHA-256, SHA512 With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Seed, Generate	Module initialization
HMAC DRBG (A3664)	SHA-256, SHA512 With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Seed, Generate	Module initialization
RSA SigVer (FIPS186-4) (A3648)	4096-bit key with SHA-256	KAT	CAST	Module becomes operational and services are	Verify	Module initialization. Before integrity test.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				available for use.		
RSA SigVer (FIPS186-4) (A3662)	4096-bit key with SHA-256	KAT	CAST	Module becomes operational and services are available for use.	Verify	Module initialization. Before integrity test.
RSA SigVer (FIPS186-4) (A3663)	4096-bit key with SHA-256	KAT	CAST	Module becomes operational and services are available for use.	Verify	Module initialization. Before integrity test.
RSA SigVer (FIPS186-4) (A3664)	4096-bit key with SHA-256	KAT	CAST	Module becomes operational and services are available for use.	Verify	Module initialization. Before integrity test.
Entropy Source	1024 samples	RCT	CAST	Module becomes operational and services are available for use.	Entropy source start-up test	Entropy source initialization
Entropy Source	1024 samples	APT	CAST	Module becomes operational and services are available for use.	Entropy source start-up test	Entropy source initialization
Entropy Source	Cutoff C = 61	RCT	CAST	Entropy source is operational	Entropy source continuous test	Continuously
Entropy Source	Cutoff C = 355	APT	CAST	Entropy source is operational	Entropy source continuous test	Continuously

Table 23: Conditional Self-Tests

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

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
HMAC-SHA2-512 (A3664)	Message Authentication	SW/FW Integrity	On demand	Manually
RSA SigVer (FIPS186-4) (A3648)	Signature Verification	SW/FW Integrity	On demand	Manually

Table 24: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
SHA-1 (A3648)	KAT	CAST	On demand	Manually
SHA-1 (A3662)	KAT	CAST	On demand	Manually
SHA-1 (A3663)	KAT	CAST	On demand	Manually
SHA-1 (A3664)	KAT	CAST	On demand	Manually
SHA2-224 (A3648)	KAT	CAST	On demand	Manually
SHA2-224 (A3662)	KAT	CAST	On demand	Manually
SHA2-224 (A3663)	KAT	CAST	On demand	Manually
SHA2-224 (A3664)	KAT	CAST	On demand	Manually
SHA2-256 (A3648)	KAT	CAST	On demand	Manually
SHA2-256 (A3662)	KAT	CAST	On demand	Manually
SHA2-256 (A3663)	KAT	CAST	On demand	Manually
SHA2-256 (A3664)	KAT	CAST	On demand	Manually
SHA2-384 (A3648)	KAT	CAST	On demand	Manually
SHA2-384 (A3662)	KAT	CAST	On demand	Manually
SHA2-384 (A3663)	KAT	CAST	On demand	Manually
SHA2-384 (A3664)	KAT	CAST	On demand	Manually
SHA2-512 (A3648)	KAT	CAST	On demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
SHA2-512 (A3662)	KAT	CAST	On demand	Manually
SHA2-512 (A3663)	KAT	CAST	On demand	Manually
SHA2-512 (A3664)	KAT	CAST	On demand	Manually
SHA3-224 (A3649)	KAT	CAST	On demand	Manually
SHA3-256 (A3649)	KAT	CAST	On demand	Manually
SHA3-384 (A3649)	KAT	CAST	On demand	Manually
SHA3-512 (A3649)	KAT	CAST	On demand	Manually
AES-ECB (A3648)	KAT	CAST	On demand	Manually
AES-ECB (A3652)	KAT	CAST	On demand	Manually
AES-ECB (A3653)	KAT	CAST	On demand	Manually
AES-ECB (A3654)	KAT	CAST	On demand	Manually
AES-ECB (A3655)	KAT	CAST	On demand	Manually
AES-ECB (A3656)	KAT	CAST	On demand	Manually
AES-ECB (A3658)	KAT	CAST	On demand	Manually
AES-ECB (A3659)	KAT	CAST	On demand	Manually
AES-ECB (A3657)	KAT	CAST	On demand	Manually
AES-CBC (A3648)	KAT	CAST	On demand	Manually
AES-CBC (A3654)	KAT	CAST	On demand	Manually
AES-CBC-CS3 (A3661)	KAT	CAST	On demand	Manually
AES-CFB128 (A3660)	KAT	CAST	On demand	Manually
AES-CTR (A3648)	KAT	CAST	On demand	Manually
AES-CTR (A3657)	KAT	CAST	On demand	Manually
AES-CCM (A3657)	KAT	CAST	On demand	Manually
AES-GCM (A3648)	KAT	CAST	On demand	Manually
AES-GCM (A3652)	KAT	CAST	On demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-GCM (A3653)	KAT	CAST	On demand	Manually
AES-GCM (A3654)	KAT	CAST	On demand	Manually
AES-GCM (A3655)	KAT	CAST	On demand	Manually
AES-GCM (A3656)	KAT	CAST	On demand	Manually
AES-GCM (A3657)	KAT	CAST	On demand	Manually
AES-GCM (A3658)	KAT	CAST	On demand	Manually
AES-GCM (A3659)	KAT	CAST	On demand	Manually
AES-XTS Testing Revision 2.0 (A3648)	KAT	CAST	On demand	Manually
AES-XTS Testing Revision 2.0 (A3657)	KAT	CAST	On demand	Manually
AES-CMAC (A3657)	KAT	CAST	On demand	Manually
HMAC-SHA-1 (A3648)	KAT	CAST	On demand	Manually
HMAC-SHA-1 (A3662)	KAT	CAST	On demand	Manually
HMAC-SHA-1 (A3663)	KAT	CAST	On demand	Manually
HMAC-SHA-1 (A3664)	KAT	CAST	On demand	Manually
HMAC-SHA2-224 (A3648)	KAT	CAST	On demand	Manually
HMAC-SHA2-224 (A3662)	KAT	CAST	On demand	Manually
HMAC-SHA2-224 (A3663)	KAT	CAST	On demand	Manually
HMAC-SHA2-224 (A3664)	KAT	CAST	On demand	Manually
HMAC-SHA2-256 (A3648)	KAT	CAST	On demand	Manually
HMAC-SHA2-256 (A3662)	KAT	CAST	On demand	Manually
HMAC-SHA2-256 (A3663)	KAT	CAST	On demand	Manually
HMAC-SHA2-256 (A3664)	KAT	CAST	On demand	Manually
HMAC-SHA2-384 (A3648)	KAT	CAST	On demand	Manually
HMAC-SHA2-384 (A3662)	KAT	CAST	On demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
HMAC-SHA2-384 (A3663)	KAT	CAST	On demand	Manually
HMAC-SHA2-384 (A3664)	KAT	CAST	On demand	Manually
HMAC-SHA2-512 (A3648)	KAT	CAST	On demand	Manually
HMAC-SHA2-512 (A3662)	KAT	CAST	On demand	Manually
HMAC-SHA2-512 (A3663)	KAT	CAST	On demand	Manually
HMAC-SHA2-512 (A3664)	KAT	CAST	On demand	Manually
HMAC-SHA3-224 (A3649)	KAT	CAST	On demand	Manually
HMAC-SHA3-256 (A3649)	KAT	CAST	On demand	Manually
HMAC-SHA3-384 (A3649)	KAT	CAST	On demand	Manually
HMAC-SHA3-512 (A3649)	KAT	CAST	On demand	Manually
Counter DRBG (A3648)	KAT	CAST	On demand	Manually
Counter DRBG (A3652)	KAT	CAST	On demand	Manually
Counter DRBG (A3653)	KAT	CAST	On demand	Manually
Counter DRBG (A3654)	KAT	CAST	On demand	Manually
Counter DRBG (A3655)	KAT	CAST	On demand	Manually
Counter DRBG (A3656)	KAT	CAST	On demand	Manually
Counter DRBG (A3657)	KAT	CAST	On demand	Manually
Counter DRBG (A3658)	KAT	CAST	On demand	Manually
Counter DRBG (A3659)	KAT	CAST	On demand	Manually
Hash DRBG (A3648)	KAT	CAST	On demand	Manually
Hash DRBG (A3652)	KAT	CAST	On demand	Manually
Hash DRBG (A3653)	KAT	CAST	On demand	Manually
Hash DRBG (A3654)	KAT	CAST	On demand	Manually
Hash DRBG (A3655)	KAT	CAST	On demand	Manually
Hash DRBG (A3656)	KAT	CAST	On demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
Hash DRBG (A3657)	KAT	CAST	On demand	Manually
Hash DRBG (A3658)	KAT	CAST	On demand	Manually
Hash DRBG (A3659)	KAT	CAST	On demand	Manually
Hash DRBG (A3662)	KAT	CAST	On demand	Manually
Hash DRBG (A3663)	KAT	CAST	On demand	Manually
Hash DRBG (A3664)	KAT	CAST	On demand	Manually
HMAC DRBG (A3648)	KAT	CAST	On demand	Manually
HMAC DRBG (A3652)	KAT	CAST	On demand	Manually
HMAC DRBG (A3653)	KAT	CAST	On demand	Manually
HMAC DRBG (A3654)	KAT	CAST	On demand	Manually
HMAC DRBG (A3655)	KAT	CAST	On demand	Manually
HMAC DRBG (A3656)	KAT	CAST	On demand	Manually
HMAC DRBG (A3657)	KAT	CAST	On demand	Manually
HMAC DRBG (A3658)	KAT	CAST	On demand	Manually
HMAC DRBG (A3659)	KAT	CAST	On demand	Manually
HMAC DRBG (A3662)	KAT	CAST	On demand	Manually
HMAC DRBG (A3663)	KAT	CAST	On demand	Manually
HMAC DRBG (A3664)	KAT	CAST	On demand	Manually
RSA SigVer (FIPS186-4) (A3648)	KAT	CAST	On demand	Manually
RSA SigVer (FIPS186-4) (A3662)	KAT	CAST	On demand	Manually
RSA SigVer (FIPS186-4) (A3663)	KAT	CAST	On demand	Manually
RSA SigVer (FIPS186-4) (A3664)	KAT	CAST	On demand	Manually
Entropy Source	RCT	CAST	On demand	Manually
Entropy Source	APT	CAST	On demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
Entropy Source	RCT	CAST	On demand	Manually
Entropy Source	APT	CAST	On demand	Manually

Table 25: Conditional Periodic Information

10.4 Error States

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

Table 26: 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 [O]

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

10.6 Additional Information [O]

Not applicable.

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

The module is distributed as a part of the Red Hat Enterprise Linux 8 (RHEL 8) package in the form of the kernel-4.18.0-372.52.1.el8_6, libkcapi-1.2.0-2.el8, and libkcapi-hmaccalc-1.2.0-2.el8 RPM packages.

The module can achieve the approved mode by:

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

In both cases, the Crypto Officer must verify the RHEL 8 system operates in the approved mode by executing the “fips-mode-setup --check” command, which should output “FIPS mode is enabled.”

11.2 Administrator Guidance

After installation of the kernel-4.18.0-372.52.1.el8_6, libkcapi-1.2.0-2.el8, and libkcapi-hmaccalc-1.2.0-2.el8 RPM packages, the Crypto Officer must execute the “cat /proc/sys/crypto/fips_name” command. The Crypto Officer must ensure that the proper name is listed in the output as follows:

Red Hat Enterprise Linux 8 - Kernel Cryptographic API

Then, the Crypto Officer must execute the “cat /proc/sys/crypto/fips_version” and “rpm -q libkcapi” commands. These commands must output the following (one line per output):

4.18.0-372.52.1.el8_6.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 [O]

Not applicable for this module.

11.5 Maintenance Requirements [O]

There are no maintenance requirements.

11.6 End of Life [O]

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-4.18.0-372.52.1.el8_6, libkcapi-1.2.0-2.el8, and libkcapi-hmaccalc-1.2.0-2.el8 RPM packages can be uninstalled from the RHEL 8 system.

11.7 Additional Information [O]

Not applicable.

12 Mitigation of Other Attacks

12.1 Attack List [O]

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

12.2 Mitigation Effectiveness [O]

Not applicable.

12.3 Guidance and Constraints [O]

Not applicable.

12.4 Additional Information [O]

Not applicable.

Appendix A. Glossary and Abbreviations

AES	Advanced Encryption Standard
API	Application Programming Interface
CAST	Cryptographic Algorithm Self-Test
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher Block Chaining
CCM	Counter with Cipher Block Chaining-Message Authentication Code
CFB	Cipher Feedback
CMAC	Cipher-based Message Authentication Code
CMVP	Cryptographic Module Validation Program
CSP	Critical Security Parameter
CTR	Counter
DRBG	Deterministic Random Bit Generator
ECB	Electronic Code Book
FIPS	Federal Information Processing Standards
GCM	Galois Counter Mode
GMAC	Galois Counter Mode Message Authentication Code
HMAC	Keyed-Hash Message Authentication Code
IPsec	Internet Protocol Security
KAT	Known Answer Test
MAC	Message Authentication Code
NIST	National Institute of Science and Technology
PAA	Processor Algorithm Acceleration
PKCS	Public-Key Cryptography Standards
RSA	Rivest, Shamir, Addleman
SHA	Secure Hash Algorithm
SSP	Sensitive Security Parameter
XTS	XEX-based Tweaked-codebook mode with cipher text Stealing

Appendix B. References

FIPS 140-3	**FIPS PUB 140-3 - Security Requirements For Cryptographic Modules** March 2019 https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-3.pdf
FIPS 140-3 IG	**Implementation Guidance for FIPS PUB 140-3 and the Cryptographic Module Validation Program** https://csrc.nist.gov/Projects/cryptographic-module-validation-program/fips-140-3-ig-announcements
FIPS 180-4	**Secure Hash Standard (SHS)** March 2012 https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf
FIPS 186-5	**Digital Signature Standard (DSS)** February 2023 https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-5.pdf
FIPS 186-4	**Digital Signature Standard (DSS)** July 2013 https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf
FIPS 198-1	**The Keyed Hash Message Authentication Code (HMAC)** July 2008 https://csrc.nist.gov/publications/fips/fips198-1/FIPS-198-1_final.pdf
FIPS 202	**SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions** August 2015 https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf
PKCS#1	**Public Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1** February 2003 https://www.ietf.org/rfc/rfc3447.txt
SP 800-38A	**Recommendation for Block Cipher Modes of Operation Methods and Techniques** December 2001 https://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf
SP 800-38B	**Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication** May 2005 https://csrc.nist.gov/publications/nistpubs/800-38B/SP_800-38B.pdf
SP 800-38C	**Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality** May 2004 https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38c.pdf
SP 800-38D	**Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC** November 2007 https://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf

SP 800-38E **Recommendation for Block Cipher Modes of Operation: The XTS AES Mode for Confidentiality on Storage Devices**
January 2010
https://csrc.nist.gov/publications/nistpubs/800-38E/nist-sp-800-38E.pdf

SP 800-90Ar1 **Recommendation for Random Number Generation Using Deterministic Random Bit Generators**
June 2015
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90Ar1.pdf