Canonical Ltd. Ubuntu 22.04 Kernel Crypto API Cryptographic Module

FIPS 140-3 Non-Proprietary Security Policy

Version 1.4

Last update: 2026-08-09

Prepared by:

atsec information security corporation

4516 Seton Center Pkwy, Suite 250

Austin, TX 78759

www.atsec.com

Table of Contents

List of Tables

List of Figures

1 General

1.1 Overview

This document is the non-proprietary FIPS 140-3 Security Policy for version 5.15.0-73-fips of the Canonical Ltd. Ubuntu 22.04 Kernel Crypto API Cryptographic 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.

1.2 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

The vendor has provided the non-proprietary Security Policy of the cryptographic module, which was further consolidated into this document by atsec information security together with other vendor-supplied documentation. In preparing the Security Policy document, the laboratory formatted the vendor-supplied documentation for consolidation without altering the technical statements therein contained. The further refining of the Security Policy document was conducted iteratively throughout the conformance testing, wherein the Security Policy was submitted to the vendor, who would then edit, modify, and add technical contents. The vendor would also supply additional documentation, which the laboratory formatted into the existing Security Policy, and resubmitted to the vendor for their final editing.

2 Cryptographic Module Specification

2.1 Description

Purpose and Use: The Canonical Ltd. Ubuntu 22.04 Kernel Crypto API Cryptographic Module (hereafter referred to as "the module") provides a C language application program interface (API) for use by other (kernel space and user space) processes that require cryptographic functionality. The module operates on a general-purpose computer as part of the Linux kernel. Its cryptographic functionality can be accessed using the Linux Kernel Crypto API.
Module Type: Software
Module Embodiment: Multi-Chip Standalone

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

Tested Operational Environment's Physical Perimeter (TOEPP): The TOEPP of the module is defined as the general-purpose computer on which the module is installed.

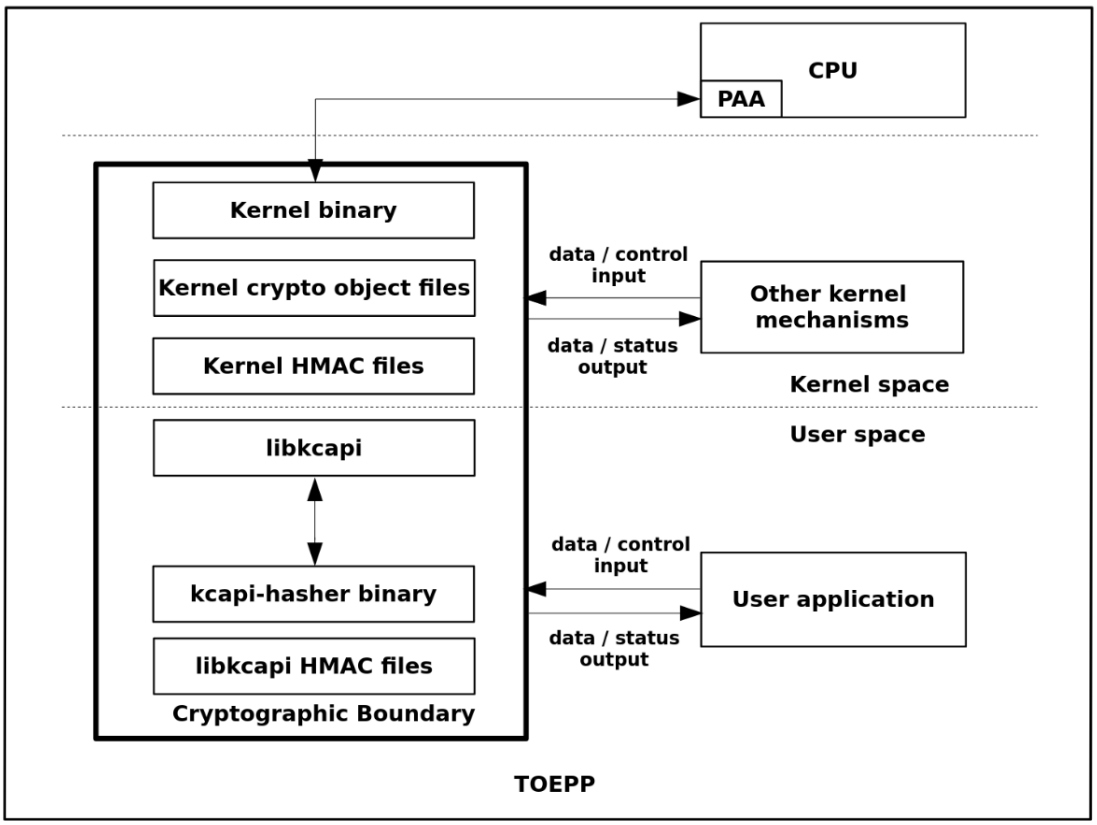

Figure 1: Block Diagram

2.2 Tested and Vendor Affirmed Module Version and Identification

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

Package or File Name	Software/ Firmware Version	Features	Integrity Test
(Supermicro SYS-1019P-WTR) /boot/vmlinuz-5.15.0-73-fips; *.ko files in /usr/lib/modules/5.15.0-73-fips/kernel/crypto/, *.ko files in /usr/lib/modules/5.15.0-73-fips/kernel/arch/x86/crypto/; /usr/lib/*-linux-gnu/libkcapi.so.1.4.0; /usr/bin/sha512hmac	kernel: 5.15.0-73-fips, libkcapi: 1.4.0-1ubuntu0.1~Fips1	N/A	HMAC-SHA2-512 (vmlinuz-5.15.0-73-fips, sha512hmac), HMAC-SHA2-256 (/usr/lib/*-linux-gnu/libkcapi.so.1.4.0), RSA signature verification with SHA2-512 and keysize of 4096 bits (.ko files)
(Amazon Web Services (AWS) c6g.metal) /boot/vmlinuz-5.15.0-73-fips; *.ko files in /usr/lib/modules/5.15.0-73-fips/kernel/crypto/, *.ko files in /usr/lib/modules/5.15.0-73-fips/kernel/arch/arm64/crypto/; /usr/lib/*-linux-gnu/libkcapi.so.1.4.0; /usr/bin/sha512hmac	kernel: 5.15.0-73-fips, libkcapi: 1.4.0-1ubuntu0.1~Fips1	N/A	HMAC-SHA2-512 (vmlinuz-5.15.0-73-fips, sha512hmac), HMAC-SHA2-256 (/usr/lib/*-linux-gnu/libkcapi.so.1.4.0), RSA signature verification with SHA2-512 and keysize of 4096 bits (.ko files)
(IBM z15) /boot/vmlinuz-5.15.0-73-fips; *.ko files in /usr/lib/modules/5.15.0-73-fips/kernel/crypto/, *.ko files in /usr/lib/modules/5.15.0-73-fips/kernel/arch/s390/crypto/; /usr/lib/*-linux-gnu/libkcapi.so.1.4.0; /usr/bin/sha512hmac	kernel: 5.15.0-73-fips, libkcapi: 1.4.0-1ubuntu0.1~Fips1	N/A	HMAC-SHA2-512 (vmlinuz-5.15.0-73-fips, sha512hmac), HMAC-SHA2-256 (/usr/lib/*-linux-gnu/libkcapi.so.1.4.0), RSA signature verification with SHA2-512 and keysize of 4096 bits (.ko files)
(Supermicro SYS-1019P-WTR) /run/mnt/kernel/kernel.efi; *.ko files in /usr/lib/modules/5.15.0-73-fips/kernel/crypto/, *.ko files in /usr/lib/modules/5.15.0-73-fips/kernel/arch/x86/crypto/; /usr/lib/*-linux-gnu/libkcapi.so.1.4.0; /usr/bin/sha512hmac	kernel: 5.15.0-73-fips, libkcapi: 1.4.0-1ubuntu0.1~Fips1	N/A	HMAC-SHA2-512 (kernel.efi, sha512hmac), HMAC-SHA2-256 (/usr/lib/*-linux-gnu/libkcapi.so.1.4.0), RSA signature verification with SHA2-512 and keysize of 4096 bits (.ko files)
(Amazon Web Services (AWS) c6g.metal) /run/mnt/kernel/kernel.efi; *.ko files in /usr/lib/modules/5.15.0-73-fips/kernel/crypto/, *.ko files in /usr/lib/modules/5.15.0-73-fips/kernel/arch/arm64/crypto/;	kernel: 5.15.0-73-fips, libkcapi: 1.4.0-1ubuntu0.1~Fips1	N/A	HMAC-SHA2-512 (kernel.efi, sha512hmac), HMAC-SHA2-256 (/usr/lib/*-linux-gnu/libkcapi.so.1.4.0), RSA signature verification with

Package or File Name	Software/ Firmware Version	Features	Integrity Test
/usr/lib/*-linux-gnu/libkcapi.so.1.4.0; /usr/bin/sha512hmac			SHA2-512 and keysize of 4096 bits (.ko files)

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:

The module makes use of hardware acceleration provided by the hardware platform. Namely, AES-NI and SHA extensions from the Intel based platform, NEON and Cryptography Extensions for the Graviton2 based platform, and CPACF for the z15 based platform, listed in the Tested Operational Environments - Software, Firmware, Hybrid table. CPACF is considered as PAI. AES-NI, SHA extensions, NEON, and Cryptography Extensions are considered as PAA.

Operating System	Hardware Platform	Processors	PAA/PAI	Hypervisor or Host OS	Version(s)
Ubuntu 22.04 LTS 64-bit	Supermicro SYS-1019P-WTR	Intel(R) Xeon(R) Gold 6226	Yes		5.15.0-73-fips
Ubuntu Core 22 64-bit	Supermicro SYS-1019P-WTR	Intel(R) Xeon(R) Gold 6226	Yes		5.15.0-73-fips
Ubuntu 22.04 LTS 64-bit	Amazon Web Services (AWS) c6g.metal	AWS Graviton2	Yes		5.15.0-73-fips
Ubuntu Core 22 64-bit	Amazon Web Services (AWS) c6g.metal	AWS Graviton2	Yes		5.15.0-73-fips
Ubuntu 22.04 LTS 64-bit	IBM z15	IBM z15	Yes		5.15.0-73-fips
Ubuntu 22.04 LTS 64-bit	Supermicro SYS-1019P-WTR	Intel(R) Xeon(R) Gold 6226	No		5.15.0-73-fips
Ubuntu Core 22 64-bit	Supermicro SYS-1019P-WTR	Intel(R) Xeon(R) Gold 6226	No		5.15.0-73-fips
Ubuntu 22.04 LTS 64-bit	Amazon Web Services (AWS) c6g.metal	AWS Graviton2	No		5.15.0-73-fips
Ubuntu Core 22 64-bit	Amazon Web Services (AWS) c6g.metal	AWS Graviton2	No		5.15.0-73-fips
Ubuntu 22.04 LTS 64-bit	IBM z15	IBM z15	No		5.15.0-73-fips

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

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

N/A for this module.

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

2.3 Excluded Components

Not applicable.

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: respective approved service function returns indicator 0.
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

Mode Change Instructions and Status:

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. 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:

Not applicable.

2.5 Algorithms

Approved Algorithms:

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	A3814, A3822, A3829, A3832, A3840, A3843, A3853, A3854, A3857	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CBC-CS3	A3819, A3828, A3838, A3849, A3853, A3854	Direction - decrypt, encrypt Key Length - 128, 192, 256 Payload Length - Payload Length: 128-65536 Increment 8	SP 800-38A
AES-CCM	A3814, A3822, A3829, A3832, A3843, A3853, A3854	Key Length - 128, 192, 256 Tag Length - 112, 128, 64, 80, 96 IV Length - IV Length: 56, 64, 72, 80, 88, 96, 104 Payload Length - Payload Length: 0-256 Increment 8 AAD Length - AAD Length: 0, 256, 65536	SP 800-38C
AES-CFB128	A3817, A3826, A3836, A3847, A3854	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A

Algorithm	CAVP Cert	Properties	Reference
AES-CMAC	A3814, A3822, A3829, A3832, A3843, A3853, A3854	Direction - Generation, Verification Key Length - 128, 192, 256 MAC Length - MAC Length: 128 Message Length - Message Length: 8-524288 Increment 8	SP 800-38B
AES-CTR	A3814, A3822, A3829, A3832, A3840, A3843, A3853, A3854, A3857	Direction - Decrypt, Encrypt Key Length - 128, 192, 256 Payload Length - Payload Length: 8-128 Increment 8 Supports Counter larger than maximum value - No Incremental Counter - Yes Counter Tests Performed - Yes	SP 800-38A
AES-ECB	A3812, A3813, A3814, A3820, A3821, A3822, A3824, A3825, A3829, A3830, A3831, A3832, A3833, A3834, A3840, A3841, A3842, A3843, A3844, A3845, A3853, A3854, A3855, A3856, A3857	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-GCM	A3814, A3822, A3829, A3832, A3843, A3854	Direction - Decrypt, Encrypt IV Generation - External IV Generation Mode - 8.2.2 Key Length - 128, 192, 256 Tag Length - 104, 112, 120, 128, 32, 64, 96 IV Length - IV Length: 96 Payload Length - Payload Length: 128-65536 Increment 128 AAD Length - AAD Length: 128, 256, 120, 0	SP 800-38D
AES-GCM	A3820, A3824, A3830, A3833, A3841, A3844, A3855	Direction - Encrypt IV Generation - Internal IV Generation Mode - 8.2.2 Key Length - 128, 192, 256 Tag Length - 128, 64, 96 IV Length - IV Length: 96 Payload Length - Payload Length: 128, 256, 120, 248 AAD Length - AAD Length: 64, 96	SP 800-38D
AES-GCM	A3821, A3825, A3831, A3834, A3840, A3842, A3845, A3856	Direction - Decrypt, Encrypt IV Generation - External IV Generation Mode - 8.2.2 Key Length - 128, 192, 256 Tag Length - 128, 64, 96 IV Length - IV Length: 96 Payload Length - Payload Length: 128, 256, 120, 248 AAD Length - AAD Length: 64, 96	SP 800-38D
AES-GMAC	A3814, A3822, A3829, A3832, A3843, A3854	Direction - Decrypt, Encrypt IV Generation - External IV Generation Mode - 8.2.2 Key Length - 128, 192, 256 Tag Length - 104, 112, 120, 128,	SP 800-38D

Algorithm	CAVP Cert	Properties	Reference
		32, 64, 96 IV Length - IV Length: 96 AAD Length - AAD Length: 128, 256, 120, 0	
AES-KW	A3815, A3823, A3835, A3846, A3854	Direction - Decrypt, Encrypt Cipher - Cipher Key Length - 128, 192, 256 Payload Length - Payload Length: 128-4096 Increment 128	SP 800-38F
AES-OFB	A3818, A3827, A3837, A3848, A3854	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-XTS Testing Revision 2.0	A3814, A3822, A3829, A3832, A3840, A3843, A3853, A3854, A3857	Direction - Decrypt, Encrypt Key Length - 128, 256 Payload Length - Payload Length: 128-65536 Increment 128 Tweak Mode - Hex Data Unit Length Matches Payload Length - Yes	SP 800-38E
Counter DRBG	A3812, A3813, A3814, A3820, A3821, A3822, A3824, A3825, A3829, A3830, A3831, A3832, A3833, A3834, A3840, A3841, A3842, A3843, A3844, A3845, A3854, A3855, A3856	Prediction Resistance - No, Yes Supports Reseed - Yes Mode - AES-128, AES-192, AES-256 Derivation Function Enabled - Yes Additional Input - Additional Input: 0 Entropy Input - Entropy Input: 128, Entropy Input: 192, Entropy Input: 256 Nonce - Nonce: 128, Nonce: 64 Personalization String Length - Personalization String Length: 0 Returned Bits - 1024, 4096, 512	SP 800-90A Rev. 1
ECDSA KeyGen (FIPS186-4)	A3813	Curve - P-256, P-384 Secret Generation Mode - Testing Candidates	FIPS 186-4
Hash DRBG	A3812, A3813, A3814, A3820, A3821, A3822, A3824, A3825, A3830, A3831, A3832, A3833, A3834, A3840, A3841, A3842, A3843, A3844, A3845, A3850, A3851, A3852, A3855, A3856	Prediction Resistance - No, Yes Supports Reseed - No Mode - SHA-1, SHA2-256, SHA2-512 Entropy Input - Entropy Input: 160, Entropy Input: 256 Nonce - Nonce: 160, Nonce: 256 Personalization String Length - Personalization String Length: 0 Additional Input - Additional Input: 0, 160, Additional Input: 0, 256 Returned Bits - 1024, 2048, 320	SP 800-90A Rev. 1
HMAC DRBG	A3812, A3813, A3814, A3820, A3821, A3822, A3824, A3825, A3830, A3831, A3832, A3833, A3834, A3840, A3841,	Prediction Resistance - No, Yes Supports Reseed - No Mode - SHA-1, SHA2-256, SHA2-512	SP 800-90A Rev. 1

Algorithm	CAVP Cert	Properties	Reference
	A3842, A3843, A3844, A3845, A3850, A3851, A3852, A3855, A3856	Entropy Input - Entropy Input: 160, Entropy Input: 256 Nonce - Nonce: 160, Nonce: 256 Personalization String Length - Personalization String Length: 0 Additional Input - Additional Input: 0, 160, Additional Input: 0, 256 Returned Bits - 1024, 2048, 320	
HMAC-SHA-1	A3812, A3813, A3814, A3832, A3850, A3851, A3852, A3853	MAC - MAC: 160 Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-224	A3812, A3813, A3814, A3832, A3850, A3851, A3852, A3853, A3857, A3858	MAC - MAC: 224 Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-256	A3812, A3813, A3814, A3832, A3850, A3851, A3852, A3853, A3857, A3858	MAC - MAC: 256 Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-384	A3812, A3813, A3814, A3832, A3850, A3851, A3852, A3858	MAC - MAC: 384 Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-512	A3812, A3813, A3814, A3832, A3850, A3851, A3852, A3858	MAC - MAC: 512 Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA3-224	A3816, A3839	MAC - MAC: 224 Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA3-256	A3816, A3839	MAC - MAC: 256 Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA3-384	A3816, A3839	MAC - MAC: 384 Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA3-512	A3816, A3839	MAC - MAC: 512 Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
KAS-ECC-SSC Sp800-56Ar3	A3813	Domain Parameter Generation Methods - P-256, P-384 Scheme - ephemeralUnified - KAS Role - initiator, responder	SP 800-56A Rev. 3
KAS-FFC-SSC Sp800-56Ar3	A3812	Domain Parameter Generation Methods - ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192 Scheme - dhEphem - KAS Role - initiator, responder	SP 800-56A Rev. 3
RSA SigVer (FIPS186-4)	A3814, A3832, A3850, A3851, A3852	Signature Type - PKCS 1.5 Modulo - 2048, 3072, 4096 Hash Pair - Hash Algorithm - SHA-1 Public Exponent Mode - Random	FIPS 186-4

Algorithm	CAVP Cert	Properties	Reference
Safe Primes Key Generation	A3812	Safe Prime Groups - ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192	SP 800-56A Rev. 3
SHA-1	A3812, A3813, A3814, A3832, A3850, A3851, A3852, A3853	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2	FIPS 180-4
SHA2-224	A3812, A3813, A3814, A3832, A3850, A3851, A3852, A3853, A3857, A3858	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2	FIPS 180-4
SHA2-256	A3812, A3813, A3814, A3832, A3850, A3851, A3852, A3853, A3857, A3858	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2	FIPS 180-4
SHA2-384	A3812, A3813, A3814, A3832, A3850, A3851, A3852, A3858	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2	FIPS 180-4
SHA2-512	A3812, A3813, A3814, A3832, A3850, A3851, A3852, A3858	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2	FIPS 180-4
SHA3-224	A3816, A3839	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2	FIPS 202
SHA3-256	A3816, A3839	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2	FIPS 202
SHA3-384	A3816, A3839	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2	FIPS 202
SHA3-512	A3816, A3839	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2	FIPS 202

Table 5: Approved Algorithms

Vendor-Affirmed Algorithms:

Name	Properties	Implementation	Reference
ECC and DH CKG	Key type:Asymmetric	N/A	SP800-133r2, section 4, example 1 (without XOR)

Table 6: Vendor-Affirmed Algorithms

Non-Approved, Allowed Algorithms:

N/A for this module.

Non-Approved, Allowed Algorithms with No Security Claimed:

N/A for this module.

Non-Approved, Not Allowed Algorithms:

Name	Use and Function
AES-GCM with external IV	Encryption (Not compliant with SP 800-38D
KBKDF (libkcapi)	Key derivation (Not CAVP tested)

Name	Use and Function
HKDF (libkcapi)	Key derivation (Not CAVP tested)
PBKDF2 (libkcapi)	Password-based key derivation (Not CAVP tested)
RSA	Encryption primitive; Decryption primitive (Not compliant to SP 800-56Br2)
RSA with PKCS#1 v1.5 padding	Signature generation (pre-hashed message); Signature verification (pre-hashed message); Key encapsulation (Not compliant to SP 800-56Br2); Key un-encapsulation (Not compliant to SP 800-56Br2)

Table 7: Non-Approved, Not Allowed Algorithms

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
Encryption and Decryption with AES	BC-UnAuth	Encryption and Decryption with AES		AES-ECB: (A3812, A3813, A3814, A3820, A3821, A3822, A3824, A3825, A3829, A3830, A3831, A3832, A3833, A3834, A3840, A3841, A3842, A3843, A3844, A3845, A3853, A3854, A3855, A3856, A3857) AES-CBC: (A3814, A3822, A3829, A3832, A3840, A3843, A3853, A3854, A3857) AES-CTR: (A3814, A3822, A3829, A3832, A3840, A3843, A3853, A3854, A3857) AES-XTS Testing Revision 2.0: (A3814, A3822, A3829, A3832, A3840, A3843, A3853, A3854, A3857) AES-KW: (A3815, A3823, A3835, A3846, A3854) AES-CFB128: (A3817, A3826, A3836, A3847, A3854) AES-OFB: (A3818, A3827, A3837, A3848, A3854) AES-CBC-CS3:

Name	Type	Description	Properties	Algorithms
				(A3819, A3828, A3838, A3849, A3853, A3854)
Random Number Generation with HMAC DRBG, Hash DRBG or Counter DRBG	DRBG	Random Number Generation with HMAC DRBG, Hash DRBG or Counter DRBG		Counter DRBG: (A3812, A3813, A3814, A3820, A3821, A3822, A3824, A3825, A3829, A3830, A3831, A3832, A3833, A3834, A3840, A3841, A3842, A3843, A3844, A3845, A3854, A3855, A3856) HMAC DRBG: (A3812, A3813, A3814, A3820, A3821, A3822, A3824, A3825, A3830, A3831, A3832, A3833, A3834, A3840, A3841, A3842, A3843, A3844, A3845, A3850, A3851, A3852, A3855, A3856) Hash DRBG: (A3812, A3813, A3814, A3820, A3821, A3822, A3824, A3825, A3830, A3831, A3832, A3833, A3834, A3840, A3841, A3842, A3843, A3844, A3845, A3850, A3851, A3852, A3855, A3856)
Message Authentication with AES	MAC	Message Authentication with AES		AES-CMAC: (A3814, A3822, A3829, A3832, A3843, A3853, A3854) AES-GMAC: (A3814, A3822, A3829, A3832, A3843, A3854)
Message Authentication with HMAC	MAC SHA	Message Authentication with HMAC		HMAC-SHA-1: (A3812, A3813, A3814, A3832, A3850, A3851, A3852, A3853)

Name	Type	Description	Properties	Algorithms
				HMAC-SHA2-224: (A3812, A3813, A3814, A3832, A3850, A3851, A3852, A3853, A3857, A3858) HMAC-SHA2-256: (A3812, A3813, A3814, A3832, A3850, A3851, A3852, A3853, A3857, A3858) HMAC-SHA2-384: (A3812, A3813, A3814, A3832, A3850, A3851, A3852, A3858) HMAC-SHA2-512: (A3812, A3813, A3814, A3832, A3850, A3851, A3852, A3858) HMAC-SHA3-224: (A3816, A3839) HMAC-SHA3-256: (A3816, A3839) HMAC-SHA3-384: (A3816, A3839) HMAC-SHA3-512: (A3816, A3839)
Shared Secret Computation with KAS-FFC-SSC or KAS-ECC-SSC	KAS-SSC	Shared Secret Computation with KAS-FFC-SSC or KAS-ECC-SSC		KAS-FFC-SSC Sp800-56Ar3: (A3812) KAS-ECC-SSC Sp800-56Ar3: (A3813)
Message Digest with SHA	SHA	Message Digest with SHA		SHA-1: (A3812, A3813, A3814, A3832, A3850, A3851, A3852, A3853) SHA2-224: (A3812, A3813, A3814, A3832, A3850, A3851, A3852, A3853, A3857, A3858) SHA2-256: (A3812, A3813, A3814, A3832, A3850, A3851, A3852, A3853, A3857, A3858) SHA2-384: (A3812, A3813, A3814,

Name	Type	Description	Properties	Algorithms
				A3832, A3850, A3851, A3852, A3858) SHA2-512: (A3812, A3813, A3814, A3832, A3850, A3851, A3852, A3858) SHA3-224: (A3816, A3839) SHA3-256: (A3816, A3839) SHA3-384: (A3816, A3839) SHA3-512: (A3816, A3839)
Key Pair Generation with ECDSA or Safe Primes	AsymKeyPair-KeyGen CKG	Key Pair Generation with ECDSA or Safe Primes		Safe Primes Key Generation: (A3812) ECDSA KeyGen (FIPS186-4): (A3813) ECC and DH CKG: ()
Authenticated Encryption and Authenticated Decryption with AES-CCM	BC-Auth	Authenticated Encryption and Authenticated Decryption with AES-CCM		AES-CCM: (A3814, A3822, A3829, A3832, A3843, A3853, A3854)
Authenticated Decryption with AES-GCM	BC-AuthDecrypt	Authenticated Decryption with AES-GCM		AES-GCM: (A3814, A3820, A3821, A3822, A3824, A3825, A3829, A3830, A3831, A3832, A3833, A3834, A3840, A3841, A3842, A3843, A3844, A3845, A3854, A3855, A3856)
Signature Verification with RSA	DigSig-SigVer SHA	Signature Verification with RSA		RSA SigVer (FIPS186-4): (A3814, A3832, A3850, A3851, A3852) SHA-1: (A3812, A3813, A3814, A3832, A3850, A3851, A3852, A3853) SHA2-224: (A3812, A3813, A3814, A3832, A3850, A3851, A3852, A3853, A3857, A3858)

Name	Type	Description	Properties	Algorithms
				SHA2-256: (A3812, A3813, A3814, A3832, A3850, A3851, A3852, A3853, A3857, A3858) SHA2-384: (A3812, A3813, A3814, A3832, A3850, A3851, A3852, A3858) SHA2-512: (A3812, A3813, A3814, A3832, A3850, A3851, A3852, A3858)
Authenticated Encryption with AES-GCM	BC-AuthEncrypt	Authenticated Encryption with AES-GCM		AES-GCM: (A3814, A3820, A3821, A3822, A3824, A3825, A3829, A3830, A3831, A3832, A3833, A3834, A3840, A3841, A3842, A3843, A3844, A3845, A3854, A3855, A3856)
Authenticated Encryption and Authenticated Decryption with AES-CBC or AES-CTR with HMAC	BC-UnAuth MAC SHA	Authenticated Encryption and Authenticated Decryption with AES-CBC or AES-CTR with HMAC		HMAC-SHA-1: (A3812, A3813, A3814, A3832, A3850, A3851, A3852, A3853) HMAC-SHA2-256: (A3812, A3813, A3814, A3832, A3850, A3851, A3852, A3853, A3857, A3858) HMAC-SHA2-384: (A3812, A3813, A3814, A3832, A3850, A3851, A3852, A3858) HMAC-SHA2-512: (A3812, A3813, A3814, A3832, A3850, A3851, A3852, A3858) AES-CBC: (A3814, A3822, A3829, A3832, A3840, A3843, A3853, A3854, A3857) AES-CTR: (A3814, A3822, A3829,

Name	Type	Description	Properties	Algorithms
				A3832, A3840, A3843, A3853, A3854, A3857) SHA-1: (A3812, A3813, A3814, A3832, A3850, A3851, A3852, A3853) SHA2-256: (A3812, A3813, A3814, A3832, A3850, A3851, A3852, A3853, A3857, A3858) SHA2-384: (A3812, A3813, A3814, A3832, A3850, A3851, A3852, A3858) SHA2-512: (A3812, A3813, A3814, A3832, A3850, A3851, A3852, A3858)

Table 8: 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 (b) 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 the *Approved Services* table.

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.

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.

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 Diffie-Hellman and EC Diffie-Hellman

The module offers DH and ECDH shared secret computation services compliant to the SP 800-56Ar3 and meeting IG D.F scenario 2 path (1). In order to meet the required assurances listed in Section 5.6 of SP 800-56Ar3, the module shall be used together with an application that implements the IPSec protocol and the following steps shall be performed:

1. The entity using the module, must use the module's "Key pair generation" service: the set_secret and generate_public_key API functions, to generate DH/ECDH ephemeral key pairs. This meets the assurances required by key pair owner defined in the section 5.6.2.1 of SP 800-56Ar3.

2. As part of the module's shared secret computation service, the module internally performs the public key validation on the peer's public key passed in as input to the API function. This meets the public key validity assurance required by the sections 5.6.2.2.1/5.6.2.2.2 of SP 800-56Ar3.

3. The module does not support static keys, therefore the "assurance of peer's possession of private key" is not applicable.

2.7.4 SHA-3

The module implements HMAC with SHA3-224, SHA3-256, SHA3-384, SHA3-512. The CAVP certificates have been obtained for the HMAC algorithm as well as for all the SHA3 implementations. The CAVP certificates are listed in the *Approved Algorithms* table.

2.7.5 RSA

The module implements FIPS 186-4 RSA SigVer. All RSA modulus lengths (i.e., 2048, 3072, 4096 bits) have been CAVP tested. The CAVP certificates are listed in the *Approved Algorithms* table.

2.7.6 SHA-1

SHA-1 is approved only when used for message authentication with HMAC or for message digest operations. The module does not support SHA-1 for signature generation or signature verification. Beginning January 1, 2031, SHA-1 will be non-approved for all purposes.

2.7.7 Key Agreement and Key Transport Schemes

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

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.

2.8 RBG and Entropy

Cert Number	Vendor Name
E59	Canonical Ltd.

Table 9: Entropy Certificates

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
Canonical Kernel CPU Time Jitter RNG Entropy source	Non-Physical	Ubuntu 22.04 LTS 64-bit on Intel(R) Xeon(R) Gold 6226 on Supermicro SYS-1019P-WTR; Ubuntu Core 22 64-bit on Intel(R) Xeon(R) Gold 6226 on Supermicro SYS-1019P-WTR; Ubuntu 22.04 LTS 64-bit on AWS Graviton2 on Amazon Web Services (AWS) c6g.metal; Ubuntu Core 22 64-bit on AWS Graviton2 on Amazon Web Services (AWS) c6g.metal; Ubuntu 22.04 LTS 64-bit on IBM z15 on IBM z15	64 bits	59.43 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, using the parameters listed specified in the *Security Function Implementations* table. 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 asymmetric key pairs). This DRBG is initially seeded with 448 output bits from the entropy source (416 bits of entropy) and reseeded with 320 output bits from the entropy source (297 bits of entropy).

The module complies with the Public Use Document for ESV certificate E59 by reading entropy data from the jent_kcapi_random() function, which corresponds to the GetEntropy()

conceptual interface. This function outputs 59 bits of entropy per 64 bit output. Outputs of multiple GetEntropy() calls are concatenated to receive the entropy input length greater than 64 bits. The output is truncated to get the entropy input string which is not a multiple of 64.

2.9 Key Generation

The module implements Cryptographic Key Generation (CKG, vendor affirmed), compliant with SP 800-133r2. When random values are required, they are directly obtained as output from the SP 800-90Ar1 approved DRBG, compliant with Section 4 of SP 800-133r2 (without XOR). The following methods are implemented:

- Safe Primes key pair generation: compliant with SP 800-133r2, Section 5.2, which maps to SP 800-56Ar3. The method described in Section 5.6.1.1.4 of SP 800-56Ar3 (“Testing Candidates”) is used.
- ECDSA key pair generation: compliant with SP 800-133r2, Section 5.1 and 5.2. The method described in Appendix B.4.2 of FIPS 186-4 (“Testing Candidates”) is used. Note that this generation method is also used to generated ECDH key pairs.

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

2.10 Key Establishment

The module implements SSP agreement and SSP transport algorithms as listed in the *Security Function Implementations* table. The module implements the following algorithms that can be used as part of a key establishment scheme:

Key agreement:

- KAS-FFC-SSC compliant with SP 800-56Ar3 and Scenario 2 (1) of FIPS 140-3 IG D.F; using ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192 safe primes groups with 112-200 bits of security strength.

- KAS-ECC-SSC compliant with SP 800-56Ar3 and Scenario 2 (1) of FIPS 140-3 IG D.F; using P-256, P-384 curves with 128, 192 bits of security strength.

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.

For Diffie-Hellman, the module supports the use of the following safe primes:

- TLS (RFC 7919): ffdhe2048 (ID = 256), ffdhe3072 (ID = 257), ffdhe4096 (ID = 258), ffdhe6144 (ID = 259), ffdhe8192 (ID = 260)

No other parts of the TLS or IPSec protocols, other than those mentioned above, have been tested by the CAVP and CMVP.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

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

Table 11: Ports and Interfaces

The logical interfaces are the APIs through which the applications request services. These logical interfaces are logically separated from each other by the API design. The module does not implement a control output interface.

4 Roles, Services, and Authentication

4.1 Authentication Methods

N/A for this module.

4.2 Roles

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

Table 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	Message Digest with SHA	Crypto Officer
Encryption	Encrypt a plaintext	crypto_skcipher_setkey returns 0	AES Key, plaintext	Ciphertext	Encryption and Decryption with AES	Crypto Officer - AES Key: W,E
Decryption	Decrypt a ciphertext	crypto_skcipher_setkey returns 0	AES Key, ciphertext	Plaintext	Encryption and Decryption with AES	Crypto Officer - AES Key: W,E
Authenticated Encryption	Encrypt a plaintext	For all except AES GCM: crypto_aead_setkey returns 0; For AES GCM: crypto_aead_get_flags(tfm) has the CRYPTO_ALG_FIPS140_COMPLIANT flag set	AES Key, IV, plaintext	Ciphertext, MAC tag	Authenticated Encryption and Authenticated Decryption with AES-CCM Authenticated Decryption with AES-GCM Authenticated Encryption with AES-GCM Authenticat	Crypto Officer - AES Key: W,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					ed Encryption and Authenticated Decryption with AES-CBC or AES-CTR with HMAC	
Authenticated Decryption	Decrypt a ciphertext	For all except AES GCM: crypto_aead_setkey returns 0; For AES GCM: crypto_aead_get_flags(tfm) has the CRYPTO_ALG_FIPS140_COMPLIANT flag set	AES key, IV, MAC tag, ciphertext	Plaintext or failure	Authenticated Encryption and Authenticated Decryption with AES-CCM Authenticated Decryption with AES-GCM Authenticated Encryption with AES-GCM Authenticated Encryption and Authenticated Decryption with AES-CBC or AES-CTR with HMAC	Crypto Officer - AES Key: W,E
Message Authentication	Compute a MAC tag	crypto_shash_init returns 0	AES Key or HMAC key, message	MAC tag	Message Authentication with AES Message Authentication with HMAC	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 HMAC DRBG, Hash DRBG or	Crypto Officer - Entropy Input: W,E - DRBG Seed: G,E - DRBG

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					Counter DRBG	Internal State (V, Key): G,W,E - DRBG Internal State (V, C): G,W,E
Shared Secret Computation	Compute a shared secret	crypto_kpp_compute_shared_secret returns 0	DH Private Key, DH public key or EC private key, EC public key	Shared secret	Shared Secret Computation with KAS-FFC-SSC or KAS-ECC-SSC	Crypto Officer - DH Public Key : W,E - DH Private Key: W,E - EC Public Key: W,E - EC Private Key: W,E - Shared Secret: G,R
Key Pair Generation	Generate a key pair	crypto_kpp_set_secret and crypto_kpp_generate_public_key return 0	Safe Primes: Group; ECDSA: Curve	Safe Primes: Module Generated DH Private Key, Module Generated DH public key; ECDSA: Module Generated EC private key, Module Generated EC public key	Key Pair Generation with ECDSA or Safe Primes	Crypto Officer - Intermediate Key Generation Value: G,E,Z - Module Generated DH Public Key : G,R - Module Generated DH Private Key: G,R - Module Generated EC Public Key: G,R - Module Generated EC Private Key: G,R
Error Detection Code	Compute an EDC (crc32, crct10dif)	None	Message	EDC	None	Crypto Officer
Compression	Compress data (deflate, lz4, lz4hc,	None	Data	Compressed data	None	Crypto Officer

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	lzo, zlib-deflate, zstd)					
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 and Decryption with AES Random Number Generation with HMAC DRBG, Hash DRBG or Counter DRBG Message Authentication with AES Message Authentication with HMAC Shared Secret Computation with KAS-FFC-SSC or KAS-ECC-SSC Message Digest with SHA Key Pair Generation with ECDSA or Safe Primes	Crypto Officer

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					Authenticated Encryption and Authenticated Decryption with AES-CCM Authenticated Decryption with AES-GCM Signature Verification with RSA Authenticated Encryption with AES-GCM Authenticated Encryption and Authenticated Decryption with AES-CBC or AES-CTR with HMAC	
Zeroization	Zeroize all SSPs	None	Any SSP	N/A	None	Crypto Officer - AES Key: Z - HMAC Key: Z - Shared Secret: Z - Entropy Input: Z - DRBG Seed: Z - DRBG Internal State (V, Key): Z - DRBG Internal State (V, C): Z - Module

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Generated DH Public Key : Z - Module Generated DH Private Key: Z - Module Generated EC Public Key: Z - Module Generated EC Private Key: Z - DH Public Key : Z - DH Private Key: Z - EC Public Key: Z - EC Private Key: Z - Intermediate Key Generation Value: Z

Table 13: 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.
- **N/A:** The module does not access any SSP or key during its operation.

4.4 Non-Approved Services

Name	Description	Algorithms	Role
AES-GCM with external IV	Encryption	AES-GCM with external IV	CO
KBKDF (libkcapi)	Key derivation	KBKDF (libkcapi)	CO
HKDF (libkcapi)	Key derivation	HKDF (libkcapi)	CO
PBKDF2 (libkcapi)	Password-based key derivation	PBKDF2 (libkcapi)	CO
RSA	Encryption primitive; Decryption primitive	RSA	CO

Name	Description	Algorithms	Role
RSA with PKCS#1 v1.5 padding	Signature generation (pre-hashed message); Signature verification (pre-hashed message); Key encapsulation; Key un-encapsulation	RSA with PKCS#1 v1.5 padding	CO

Table 14: Non-Approved Services

4.5 External Software/Firmware Loaded

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 SHA2-512 implementations). The HMAC key used is located within the sha512hmac binary. The kernel crypto object files listed in the *Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets)* table are loaded on start-up by the module and verified using RSA signature verification with PKCS#1 v1.5 padding, SHA2-512, and a 4096-bit key. The RSA key used is located within the kernel binary.

The libkcapi and sha512hmac software components perform their own internal integrity test, respectively using the HMAC-SHA2-256 and HMAC-SHA2-512 implementations provided by the Linux kernel.

5.2 Initiate on Demand

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

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Modifiable

How Requirements are Satisfied: The module executes as part of a general-purpose operating system (Canonical Ubuntu 22.04 and Canonical Ubuntu Core 22), which allows modification, loading, and execution of software that is not part of the validated module.

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

6.2 Configuration Settings and Restrictions

The module shall be installed as specified in Section 11.1.

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

7 Physical Security

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

8 Non-Invasive Security

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

9 Sensitive Security Parameters Management

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
RAM	Temporary storage for SSPs used by the module as part of service execution. The module does not perform persistent storage of SSPs	Dynamic

Table 15: Storage Areas

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

9.2 SSP Input-Output Methods

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

Table 16: SSP Input-Output Methods

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Wipe and Free memory block allocated	Zeroizes the SSPs contained within the cipher handle.	Memory occupied by SSPs is overwritten with zeroes and then it is released, which renders the SSP values irretrievable. The completion of the zeroization routine indicates that the zeroization procedure succeeded.	By calling the cipher related zeroization API
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
Module Reset	De-allocates the volatile memory used to store SSPs	Volatile memory used by the module is overwritten within nanoseconds when power is removed.	By unloading and reloading the module

Table 17: SSP Zeroization Methods

All data output is inhibited during zeroization.

9.4 SSPs

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
AES Key	AES key used for Encryption; Decryption; Authenticated encryption; Authenticated decryption; Message authentication;	XTS: 128, 256 bits; Other modes: 128, 192, 256 bits - XTS: 128, 256 bits; Other modes: 128, 192, 256 bits	Symmetric key - CSP			Encryption and Decryption with AES Message Authentication with AES
HMAC Key	HMAC key used for Message authentication code (MAC);	112-524288 bits - 112-256 bits	Symmetric key - CSP			Message Authentication with HMAC
Shared Secret	Shared secret established during Shared Secret Computation	KAS-FFC-SSC: ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192; KAS-ECC-SSC: P-256, P-384 - KAS-FFC-SSC: 112-200 bits; KAS-ECC-SSC: 128, 192 bits	Shared secret - CSP		Shared Secret Computation with KAS-FFC-SSC or KAS-ECC-SSC	
Entropy Input	Entropy input used to seed the DRBGs	128-448 bits - 128-256 bits	Entropy input - CSP			Random Number Generation with HMAC DRBG, Hash DRBG or Counter DRBG
DRBG Seed	DRBG seed derived from Entropy Input	Counter DRBG: 256, 320, 384 bits; Hash_DRBG: 440, 888 bits; HMAC DRBG: 160, 256, 512 bits - Counter DRBG: 128, 192, 256 bits; Hash DRBG: 128, 256 bits; HMAC DRBG: 128, 256 bits	Seed - CSP	Random Number Generation with HMAC DRBG, Hash DRBG or Counter DRBG		Random Number Generation with HMAC DRBG, Hash DRBG or Counter DRBG
DRBG Internal State (V, Key)	Internal state of Counter DRBG and HMAC DRBG instances	Counter DRBG: 256, 320, 348 bits; HMAC DRBG: 320, 512,	Internal state - CSP	Random Number Generation with HMAC DRBG, Hash		Random Number Generation with HMAC DRBG, Hash

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
		1024 bits - Counter DRBG: 128, 192, 256 bits; HMAC DRBG: 128, 256 bits		DRBG or Counter DRBG		DRBG or Counter DRBG
DRBG Internal State (V, C)	Internal state of Hash DRBG instance	440, 888 bits - 128, 256 bits	Internal state - CSP	Random Number Generation with HMAC DRBG, Hash DRBG or Counter DRBG		Random Number Generation with HMAC DRBG, Hash DRBG or Counter DRBG
DH Public Key	Public key used for KAS-FFC-SSC	ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192 - 112-200 bits	Public key - PSP			Shared Secret Computation with KAS-FFC-SSC or KAS-ECC-SSC
DH Private Key	DH private key used for KAS-FFC-SSC	ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192 - 112-200 bits	Private key - CSP			Shared Secret Computation with KAS-FFC-SSC or KAS-ECC-SSC
EC Public Key	Public key used for KAS-ECC-SSC	P-256, P-384 - 128, 192 bits	Public key - PSP			Shared Secret Computation with KAS-FFC-SSC or KAS-ECC-SSC
EC Private Key	EC private key used for KAS-ECC-SSC	P-256, P-384 - 128, 192 bits	Private key - CSP			Shared Secret Computation with KAS-FFC-SSC or KAS-ECC-SSC
Module Generated DH Public Key	DH public key	ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192 - 112-200 bits	Public key - PSP	Key Pair Generation with ECDSA or Safe Primes		
Module Generated DH Private Key	DH private key	ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192 - 112-200 bits	Private key - CSP	Key Pair Generation with ECDSA or Safe Primes		
Module Generated EC Public Key	EC public key	P-256, P-384 - 128, 192 bits	Public key - PSP	Key Pair Generation with ECDSA or Safe Primes		

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
Module Generated EC Private Key	EC private key	P-256, P-384 - 128, 192 bits	Private key - CSP	Key Pair Generation with ECDSA or Safe Primes		
Intermediate Key Generation Value	Intermediate value generated during Key Pair Generation	2048-8192 bits - 112-200 bits	Intermediate value - CSP	Key Pair Generation with ECDSA or Safe Primes		Key Pair Generation with ECDSA or Safe Primes

Table 18: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
AES Key	API input parameters; AF_ALG_type sockets (input)	RAM:Plaintext	From service invocation to service completion	Wipe and Free memory block allocated	
HMAC Key	API input parameters; AF_ALG_type sockets (input)	RAM:Plaintext	From service invocation to service completion	Wipe and Free memory block allocated	
Shared Secret	API output parameters; AF_ALG type sockets (output)	RAM:Plaintext	From service invocation to service completion	Wipe and Free memory block allocated	DH Public Key :Derived From EC Public Key:Derived From
Entropy Input		RAM:Plaintext	From service invocation to service completion	Automatic Module Reset	DRBG Seed:Derives
DRBG Seed		RAM:Plaintext	From service invocation to service completion	Automatic Module Reset	Entropy Input:Derived From DRBG Internal State (V, Key):Derives DRBG Internal State (V, C):Derives
DRBG Internal State (V, Key)		RAM:Plaintext	From service invocation to service completion	Wipe and Free memory block allocated	DRBG Seed:Derived From
DRBG Internal State (V, C)		RAM:Plaintext	From service invocation to service completion	Wipe and Free memory block allocated	DRBG Seed:Derived From
DH Public Key	API input parameters; AF_ALG_type sockets (input) API output parameters; AF_ALG type sockets (output)	RAM:Plaintext	From service invocation to service completion	Wipe and Free memory block allocated	Module Generated DH Private Key:Paired With Shared Secret:Derives Intermediate Key Generation Value:Generated From

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
DH Private Key	API input parameters; AF_ALG_type sockets (input) API output parameters; AF_ALG type sockets (output)	RAM:Plaintext	From service invocation to service completion	Wipe and Free memory block allocated	Module Generated DH Public Key :Paired With Shared Secret:Derives Intermediate Key Generation Value:Generated From
EC Public Key	API input parameters; AF_ALG_type sockets (input) API output parameters; AF_ALG type sockets (output)	RAM:Plaintext	From service invocation to service completion	Wipe and Free memory block allocated	EC Private Key:Paired With Shared Secret:Derives Intermediate Key Generation Value:Generated From
EC Private Key	API input parameters; AF_ALG_type sockets (input) API output parameters; AF_ALG type sockets (output)	RAM:Plaintext	From service invocation to service completion	Wipe and Free memory block allocated	EC Public Key:Paired With Shared Secret:Derives Intermediate Key Generation Value:Generated From
Module Generated DH Public Key	API output parameters; AF_ALG type sockets (output)	RAM:Plaintext	From service invocation to service completion	Wipe and Free memory block allocated	Module Generated DH Private Key:Paired With Intermediate Key Generation Value:Generated From
Module Generated DH Private Key	API output parameters; AF_ALG type sockets (output)	RAM:Plaintext	From service invocation to service completion	Wipe and Free memory block allocated	Module Generated DH Public Key :Paired With Intermediate Key Generation Value:Generated From
Module Generated EC Public Key	API output parameters; AF_ALG type sockets (output)	RAM:Plaintext	From service invocation to service completion	Wipe and Free memory block allocated	EC Private Key:Paired With Shared Secret:Derives Intermediate Key Generation Value:Generated From
Module Generated EC Private Key	API output parameters; AF_ALG type sockets (output)	RAM:Plaintext	From service invocation to service completion	Wipe and Free memory block allocated	EC Public Key:Paired With Shared Secret:Derives Intermediate Key Generation

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
					Value:Generated From
Intermediate Key Generation Value		RAM:Plaintext	From service invocation to service completion	Automatic	Module Generated DH Public Key :Generates Module Generated DH Private Key:Generates Module Generated EC Public Key:Generates Module Generated EC Private Key:Generates

Table 19: SSP Table 2

The Entropy Input, DRBG Seed values, and DRBG Internal States are compliant with FIPS IG D.L.

9.5 Transitions

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

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

10 Self-Tests

10.1 Pre-Operational Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
HMAC-SHA2-256 (A3852) - x86 libkcapi	128-bit key	Message Authentication	SW/FW Integrity	Module becomes operational and services are available for use	Used for libkcapi binary
HMAC-SHA2-512 (A3852) - x86 kernel	128-bit key	Message Authentication	SW/FW Integrity	Module becomes operational and services are available for use	Used for kernel binary
HMAC-SHA2-512 (A3852) - x86 sha512hmac	128-bit key	Message Authentication	SW/FW Integrity	Module becomes operational and services are available for use	Used for sha512hmac binary
HMAC-SHA2-256 (A3832) - s390 libkcapi	128-bit key	Message Authentication	SW/FW Integrity	Module becomes operational and services are available for use	Used for libkcapi binary
HMAC-SHA2-512 (A3832) - s390 kernel	128-bit key	Message Authentication	SW/FW Integrity	Module becomes operational and services are available for use	Used for kernel binary
HMAC-SHA2-512 (A3832) - s390 sha512hmac	128-bit key	Message Authentication	SW/FW Integrity	Module becomes operational and services are available for use	Used for sha512hmac binary
HMAC-SHA2-256 (A3858) - arm libkcapi	128-bit key	Message Authentication	SW/FW Integrity	Module becomes operational and services are available for use	Used for libkcapi binary
HMAC-SHA2-512 (A3858) - arm kernel	128-bit key	Message Authentication	SW/FW Integrity	Module becomes operational and services are available for use	Used for kernel binary
HMAC-SHA2-512 (A3858) - arm sha512hmac	128-bit key	Message Authentication	SW/FW Integrity	Module becomes operational and services are available for use	Used for sha512hmac binary
RSA SigVer (FIPS186-4) (A3852) - x86 .ko files	4096-bit key with SHA2-512	Signature Verification	SW/FW Integrity	Module becomes operational and services are available for use	Used for kernel modules
RSA SigVer (FIPS186-4) (A3832) - s390 .ko files	4096-bit key with SHA2-512	Signature Verification	SW/FW Integrity	Module becomes operational and services are available for use	Used for kernel modules
RSA SigVer (FIPS186-4)	4096-bit key with SHA2-512	Signature Verification	SW/FW Integrity	Module becomes operational and	Used for kernel modules

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
(A3814) - arm .ko files				services are available for use	

Table 20: Pre-Operational Self-Tests

The pre-operational software integrity tests are performed automatically when the module is powered on, before the module transitions into the operational state. While the module is executing the self-tests, services are not available, and data output (via the data output interface) is inhibited until the tests are successfully completed. The module transitions to the operational state only after the pre-operational self-tests are passed successfully.

10.2 Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-ECB (A3812) - Encrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3813) - Encrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3814) - Encrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3820) - Encrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3821) - Encrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3822) - Encrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3824) - Encrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3825) - Encrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3829) - Encrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-ECB (A3830) - Encrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3831) - Encrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3832) - Encrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3833) - Encrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3834) - Encrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3840) - Encrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3841) - Encrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3842) - Encrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3843) - Encrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3844) - Encrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3845) - Encrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3853) - Encrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3854) - Encrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-ECB (A3855) - Encrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3856) - Encrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3857) - Encrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CBC (A3814) - Encrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CBC (A3822) - Encrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CBC (A3829) - Encrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CBC (A3832) - Encrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CBC (A3840) - Encrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CBC (A3843) - Encrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CBC (A3853) - Encrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CBC (A3854) - Encrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CBC (A3857) - Encrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CBC-CS3 (A3819) - Encrypt	128 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-CBC-CS3 (A3828) - Encrypt	128 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CBC-CS3 (A3838) - Encrypt	128 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CBC-CS3 (A3849) - Encrypt	128 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CBC-CS3 (A3853) - Encrypt	128 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CBC-CS3 (A3854) - Encrypt	128 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CFB128 (A3817) - Encrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CFB128 (A3826) - Encrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CFB128 (A3836) - Encrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CFB128 (A3847) - Encrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CFB128 (A3854) - Encrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CTR (A3814) - Encrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CTR (A3822) - Encrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CTR (A3829) - Encrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-CTR (A3832) - Encrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CTR (A3840) - Encrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CTR (A3843) - Encrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CTR (A3853) - Encrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CTR (A3854) - Encrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CTR (A3857) - Encrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CCM (A3814) - Encrypt	128, 192, 256 bit keys, 128-bit IVs	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CCM (A3822) - Encrypt	128, 192, 256 bit keys, 128-bit IVs	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CCM (A3829) - Encrypt	128, 192, 256 bit keys, 128-bit IVs	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CCM (A3832) - Encrypt	128, 192, 256 bit keys, 128-bit IVs	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CCM (A3843) - Encrypt	128, 192, 256 bit keys, 128-bit IVs	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CCM (A3853) - Encrypt	128, 192, 256 bit keys, 128-bit IVs	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CCM (A3854) - Encrypt	128, 192, 256 bit keys, 128-bit IVs	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-GCM (A3814) - Encrypt	128, 192, 256 bit keys, 96-bit (internal IV)	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3820) - Encrypt	128, 192, 256 bit keys, 96-bit (internal IV)	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3821) - Encrypt	128, 192, 256 bit keys, 96-bit (internal IV)	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3822) - Encrypt	128, 192, 256 bit keys, 96-bit (internal IV)	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3824) - Encrypt	128, 192, 256 bit keys, 96-bit (internal IV)	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3825) - Encrypt	128, 192, 256 bit keys, 96-bit (internal IV)	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3829) - Encrypt	128, 192, 256 bit keys, 96-bit (internal IV)	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3830) - Encrypt	128, 192, 256 bit keys, 96-bit (internal IV)	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3831) - Encrypt	128, 192, 256 bit keys, 96-bit (internal IV)	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3832) - Encrypt	128, 192, 256 bit keys, 96-bit (internal IV)	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3833) - Encrypt	128, 192, 256 bit keys, 96-bit (internal IV)	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3834) - Encrypt	128, 192, 256 bit keys, 96-bit (internal IV)	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3840) - Encrypt	128, 192, 256 bit keys, 96-bit (internal IV)	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-GCM (A3841) - Encrypt	128, 192, 256 bit keys, 96-bit (internal IV)	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3842) - Encrypt	128, 192, 256 bit keys, 96-bit (internal IV)	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3843) - Encrypt	128, 192, 256 bit keys, 96-bit (internal IV)	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3844) - Encrypt	128, 192, 256 bit keys, 96-bit (internal IV)	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3845) - Encrypt	128, 192, 256 bit keys, 96-bit (internal IV)	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3854) - Encrypt	128, 192, 256 bit keys, 96-bit (internal IV)	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3855) - Encrypt	128, 192, 256 bit keys, 96-bit (internal IV)	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3856) - Encrypt	128, 192, 256 bit keys, 96-bit (internal IV)	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-KW (A3815) - Encrypt	128 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-KW (A3823) - Encrypt	128 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-KW (A3835) - Encrypt	128 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-KW (A3846) - Encrypt	128 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-OFB (A3818) - Encrypt	128 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-OFB (A3827) - Encrypt	128 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-OFB (A3837) - Encrypt	128 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-OFB (A3848) - Encrypt	128 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-OFB (A3854) - Encrypt	128 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-XTS Testing Revision 2.0 (A3814) - Encrypt	128 and 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-XTS Testing Revision 2.0 (A3822) - Encrypt	128 and 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-XTS Testing Revision 2.0 (A3829) - Encrypt	128 and 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-XTS Testing Revision 2.0 (A3832) - Encrypt	128 and 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-XTS Testing Revision 2.0 (A3840) - Encrypt	128 and 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-XTS Testing Revision 2.0 (A3843) - Encrypt	128 and 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-XTS Testing Revision 2.0 (A3853) - Encrypt	128 and 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-XTS Testing Revision 2.0 (A3854) - Encrypt	128 and 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-XTS Testing Revision 2.0 (A3857) - Encrypt	128 and 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3812) - Decrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3813) - Decrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3814) - Decrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3820) - Decrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3821) - Decrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3822) - Decrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3824) - Decrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3825) - Decrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3829) - Decrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3830) - Decrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3831) - Decrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
						before the integrity test
AES-ECB (A3832) - Decrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3833) - Decrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3834) - Decrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3840) - Decrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3841) - Decrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3842) - Decrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3843) - Decrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3844) - Decrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3845) - Decrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3853) - Decrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3854) - Decrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3855) - Decrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3856) - Decrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
						before the integrity test
AES-ECB (A3857) - Decrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CBC (A3814) - Decrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CBC (A3822) - Decrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CBC (A3829) - Decrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CBC (A3832) - Decrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CBC (A3840) - Decrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CBC (A3843) - Decrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CBC (A3853) - Decrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CBC (A3854) - Decrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CBC (A3857) - Decrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CBC-CS3 (A3819) - Decrypt	128 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CBC-CS3 (A3828) - Decrypt	128 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CBC-CS3 (A3838) - Decrypt	128 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
						before the integrity test
AES-CBC-CS3 (A3849) - Decrypt	128 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CBC-CS3 (A3853) - Decrypt	128 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CBC-CS3 (A3854) - Decrypt	128 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CFB128 (A3817) - Decrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CFB128 (A3826) - Decrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CFB128 (A3836) - Decrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CFB128 (A3847) - Decrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CFB128 (A3854) - Decrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CTR (A3814) - Decrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CTR (A3822) - Decrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CTR (A3829) - Decrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CTR (A3832) - Decrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CTR (A3840) - Decrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
						before the integrity test
AES-CTR (A3843) - Decrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CTR (A3853) - Decrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CTR (A3854) - Decrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CTR (A3857) - Decrypt	128, 192, 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CCM (A3814) - Decrypt	128, 192, 256 bit keys, 128-bit IVs	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CCM (A3822) - Decrypt	128, 192, 256 bit keys, 128-bit IVs	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CCM (A3829) - Decrypt	128, 192, 256 bit keys, 128-bit IVs	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CCM (A3832) - Decrypt	128, 192, 256 bit keys, 128-bit IVs	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CCM (A3843) - Decrypt	128, 192, 256 bit keys, 128-bit IVs	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CCM (A3853) - Decrypt	128, 192, 256 bit keys, 128-bit IVs	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CCM (A3854) - Decrypt	128, 192, 256 bit keys, 128-bit IVs	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3814) - Decrypt	128, 192, 256 bit keys, 96-bit (internal IV)	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3820) - Decrypt	128, 192, 256 bit keys, 96-bit (internal IV)	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
						before the integrity test
AES-GCM (A3821) - Decrypt	128, 192, 256 bit keys, 96-bit (internal IV)	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3822) - Decrypt	128, 192, 256 bit keys, 96-bit (internal IV)	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3824) - Decrypt	128, 192, 256 bit keys, 96-bit (internal IV)	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3825) - Decrypt	128, 192, 256 bit keys, 96-bit (internal IV)	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3829) - Decrypt	128, 192, 256 bit keys, 96-bit (internal IV)	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3830) - Decrypt	128, 192, 256 bit keys, 96-bit (internal IV)	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3831) - Decrypt	128, 192, 256 bit keys, 96-bit (internal IV)	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3832) - Decrypt	128, 192, 256 bit keys, 96-bit (internal IV)	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3833) - Decrypt	128, 192, 256 bit keys, 96-bit (internal IV)	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3834) - Decrypt	128, 192, 256 bit keys, 96-bit (internal IV)	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3840) - Decrypt	128, 192, 256 bit keys, 96-bit (internal IV)	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3841) - Decrypt	128, 192, 256 bit keys, 96-bit (internal IV)	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3842) - Decrypt	128, 192, 256 bit keys, 96-bit (internal IV)	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
						before the integrity test
AES-GCM (A3843) - Decrypt	128, 192, 256 bit keys, 96-bit (internal IV)	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3844) - Decrypt	128, 192, 256 bit keys, 96-bit (internal IV)	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3845) - Decrypt	128, 192, 256 bit keys, 96-bit (internal IV)	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3854) - Decrypt	128, 192, 256 bit keys, 96-bit (internal IV)	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3855) - Decrypt	128, 192, 256 bit keys, 96-bit (internal IV)	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3856) - Decrypt	128, 192, 256 bit keys, 96-bit (internal IV)	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-KW (A3815) - Decrypt	128 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-KW (A3823) - Decrypt	128 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-KW (A3835) - Decrypt	128 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-KW (A3846) - Decrypt	128 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-OFB (A3818) - Decrypt	128 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-OFB (A3827) - Decrypt	128 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-OFB (A3837) - Decrypt	128 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
						before the integrity test
AES-OFB (A3848) - Decrypt	128 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-OFB (A3854) - Decrypt	128 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-XTS Testing Revision 2.0 (A3814) - Decrypt	128 and 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-XTS Testing Revision 2.0 (A3822) - Decrypt	128 and 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-XTS Testing Revision 2.0 (A3829) - Decrypt	128 and 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-XTS Testing Revision 2.0 (A3832) - Decrypt	128 and 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-XTS Testing Revision 2.0 (A3840) - Decrypt	128 and 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-XTS Testing Revision 2.0 (A3843) - Decrypt	128 and 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-XTS Testing Revision 2.0 (A3853) - Decrypt	128 and 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-XTS Testing Revision 2.0 (A3854) - Decrypt	128 and 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-XTS Testing Revision 2.0	128 and 256 bit keys	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
(A3857) - Decrypt						before the integrity test
AES-CMAC (A3814)	128 and 256 bit keys, encrypt	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
AES-CMAC (A3822)	128 and 256 bit keys, encrypt	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
AES-CMAC (A3829)	128 and 256 bit keys, encrypt	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
AES-CMAC (A3832)	128 and 256 bit keys, encrypt	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
AES-CMAC (A3843)	128 and 256 bit keys, encrypt	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
AES-CMAC (A3853)	128 and 256 bit keys, encrypt	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
AES-CMAC (A3854)	128 and 256 bit keys, encrypt	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
SHA-1 (A3812)	SHA-1	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA-1 (A3813)	SHA-1	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA-1 (A3814)	SHA-1	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA-1 (A3832)	SHA-1	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA-1 (A3850)	SHA-1	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA-1 (A3851)	SHA-1	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
						before the integrity test
SHA-1 (A3852)	SHA-1	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA-1 (A3853)	SHA-1	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-224 (A3812)	SHA2-224	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-224 (A3813)	SHA2-224	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-224 (A3814)	SHA2-224	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-224 (A3832)	SHA2-224	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-224 (A3850)	SHA2-224	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-224 (A3851)	SHA2-224	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-224 (A3852)	SHA2-224	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-224 (A3853)	SHA2-224	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-224 (A3857)	SHA2-224	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-224 (A3858)	SHA2-224	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-256 (A3812)	SHA2-256	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
						before the integrity test
SHA2-256 (A3813)	SHA2-256	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-256 (A3814)	SHA2-256	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-256 (A3832)	SHA2-256	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-256 (A3850)	SHA2-256	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-256 (A3851)	SHA2-256	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-256 (A3852)	SHA2-256	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-256 (A3853)	SHA2-256	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-256 (A3857)	SHA2-256	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-256 (A3858)	SHA2-256	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-384 (A3812)	SHA2-384	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-384 (A3813)	SHA2-384	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-384 (A3814)	SHA2-384	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-384 (A3832)	SHA2-384	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
						before the integrity test
SHA2-384 (A3850)	SHA2-384	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-384 (A3851)	SHA2-384	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-384 (A3852)	SHA2-384	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-384 (A3858)	SHA2-384	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-512 (A3812)	SHA2-512	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-512 (A3813)	SHA2-512	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-512 (A3814)	SHA2-512	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-512 (A3832)	SHA2-512	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-512 (A3850)	SHA2-512	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-512 (A3851)	SHA2-512	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-512 (A3852)	SHA2-512	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-512 (A3858)	SHA2-512	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA3-224 (A3816)	SHA3-224	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
						before the integrity test
SHA3-224 (A3839)	SHA3-224	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA3-256 (A3816)	SHA3-256	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA3-256 (A3839)	SHA3-256	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA3-384 (A3816)	SHA3-384	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA3-384 (A3839)	SHA3-384	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA3-512 (A3816)	SHA3-512	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA3-512 (A3839)	SHA3-512	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
HMAC-SHA-1 (A3812)	SHA-1	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA-1 (A3813)	SHA-1	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA-1 (A3814)	SHA-1	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA-1 (A3832)	SHA-1	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA-1 (A3850)	SHA-1	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA-1 (A3851)	SHA-1	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
						before the integrity test
HMAC-SHA-1 (A3852)	SHA-1	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA-1 (A3853)	SHA-1	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-224 (A3812)	SHA2-224	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-224 (A3813)	SHA2-224	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-224 (A3814)	SHA2-224	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-224 (A3832)	SHA2-224	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-224 (A3850)	SHA2-224	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-224 (A3851)	SHA2-224	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-224 (A3852)	SHA2-224	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-224 (A3853)	SHA2-224	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-224 (A3857)	SHA2-224	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-224 (A3858)	SHA2-224	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-256 (A3812)	SHA2-256	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
						before the integrity test
HMAC-SHA2-256 (A3813)	SHA2-256	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-256 (A3814)	SHA2-256	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-256 (A3832)	SHA2-256	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-256 (A3850)	SHA2-256	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-256 (A3851)	SHA2-256	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-256 (A3852)	SHA2-256	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-256 (A3853)	SHA2-256	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-256 (A3857)	SHA2-256	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-256 (A3858)	SHA2-256	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-384 (A3812)	SHA2-384	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-384 (A3813)	SHA2-384	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-384 (A3814)	SHA2-384	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-384 (A3832)	SHA2-384	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
						before the integrity test
HMAC-SHA2-384 (A3850)	SHA2-384	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-384 (A3851)	SHA2-384	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-384 (A3852)	SHA2-384	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-384 (A3858)	SHA2-384	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-512 (A3812)	SHA2-512	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-512 (A3813)	SHA2-512	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-512 (A3814)	SHA2-512	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-512 (A3832)	SHA2-512	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-512 (A3850)	SHA2-512	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-512 (A3851)	SHA2-512	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-512 (A3852)	SHA2-512	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-512 (A3858)	SHA2-512	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA3-224 (A3816)	SHA3-224	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
						before the integrity test
HMAC-SHA3-224 (A3839)	SHA3-224	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA3-256 (A3816)	SHA3-256	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA3-256 (A3839)	SHA3-256	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA3-384 (A3816)	SHA3-384	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA3-384 (A3839)	SHA3-384	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA3-512 (A3816)	SHA3-512	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA3-512 (A3839)	SHA3-512	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
Counter DRBG (A3812)	128, 192, 256 bit keys, with/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
Counter DRBG (A3813)	128, 192, 256 bit keys, with/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
Counter DRBG (A3814)	128, 192, 256 bit keys, with/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
Counter DRBG (A3820)	128, 192, 256 bit keys, with/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
Counter DRBG (A3821)	128, 192, 256 bit keys, with/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
Counter DRBG (A3822)	128, 192, 256 bit keys, with/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate,	Test runs at power-on

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
					reseed, generate) health test	before the integrity test
Counter DRBG (A3824)	128, 192, 256 bit keys, with/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
Counter DRBG (A3825)	128, 192, 256 bit keys, with/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
Counter DRBG (A3829)	128, 192, 256 bit keys, with/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
Counter DRBG (A3830)	128, 192, 256 bit keys, with/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
Counter DRBG (A3831)	128, 192, 256 bit keys, with/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
Counter DRBG (A3832)	128, 192, 256 bit keys, with/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
Counter DRBG (A3833)	128, 192, 256 bit keys, with/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
Counter DRBG (A3834)	128, 192, 256 bit keys, with/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
Counter DRBG (A3840)	128, 192, 256 bit keys, with/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
Counter DRBG (A3841)	128, 192, 256 bit keys, with/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
Counter DRBG (A3842)	128, 192, 256 bit keys, with/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
Counter DRBG (A3843)	128, 192, 256 bit keys, with/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
Counter DRBG (A3844)	128, 192, 256 bit keys, with/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate,	Test runs at power-on

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
					reseed, generate) health test	before the integrity test
Counter DRBG (A3845)	128, 192, 256 bit keys, with/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
Counter DRBG (A3854)	128, 192, 256 bit keys, with/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
Counter DRBG (A3855)	128, 192, 256 bit keys, with/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
Counter DRBG (A3856)	128, 192, 256 bit keys, with/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
Hash DRBG (A3812)	SHA2-256 With/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
Hash DRBG (A3813)	SHA2-256 With/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
Hash DRBG (A3814)	SHA2-256 With/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
Hash DRBG (A3820)	SHA2-256 With/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
Hash DRBG (A3821)	SHA2-256 With/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
Hash DRBG (A3822)	SHA2-256 With/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
Hash DRBG (A3824)	SHA2-256 With/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
Hash DRBG (A3825)	SHA2-256 With/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
Hash DRBG (A3830)	SHA2-256 With/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate,	Test runs at power-on

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
					reseed, generate) health test	before the integrity test
Hash DRBG (A3831)	SHA2-256 With/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
Hash DRBG (A3832)	SHA2-256 With/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
Hash DRBG (A3833)	SHA2-256 With/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
Hash DRBG (A3834)	SHA2-256 With/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
Hash DRBG (A3840)	SHA2-256 With/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
Hash DRBG (A3841)	SHA2-256 With/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
Hash DRBG (A3842)	SHA2-256 With/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
Hash DRBG (A3843)	SHA2-256 With/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
Hash DRBG (A3844)	SHA2-256 With/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
Hash DRBG (A3845)	SHA2-256 With/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
Hash DRBG (A3850)	SHA2-256 With/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
Hash DRBG (A3851)	SHA2-256 With/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
Hash DRBG (A3852)	SHA2-256 With/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate,	Test runs at power-on

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
					reseed, generate) health test	before the integrity test
Hash DRBG (A3855)	SHA2-256 With/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
Hash DRBG (A3856)	SHA2-256 With/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
HMAC DRBG (A3812)	HMAC-SHA2-256, HMAC-SHA2-512, with/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
HMAC DRBG (A3813)	HMAC-SHA2-256, HMAC-SHA2-512, with/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
HMAC DRBG (A3814)	HMAC-SHA2-256, HMAC-SHA2-512, with/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
HMAC DRBG (A3820)	HMAC-SHA2-256, HMAC-SHA2-512, with/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
HMAC DRBG (A3821)	HMAC-SHA2-256, HMAC-SHA2-512, with/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
HMAC DRBG (A3822)	HMAC-SHA2-256, HMAC-SHA2-512, with/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
HMAC DRBG (A3824)	HMAC-SHA2-256, HMAC-SHA2-512, with/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
HMAC DRBG (A3825)	HMAC-SHA2-256, HMAC-SHA2-512, with/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
HMAC DRBG (A3830)	HMAC-SHA2-256, HMAC-SHA2-512, with/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
HMAC DRBG (A3831)	HMAC-SHA2-256, HMAC-SHA2-512, with/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
HMAC DRBG (A3832)	HMAC-SHA2-256, HMAC-SHA2-512, with/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate,	Test runs at power-on

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
					reseed, generate) health test	before the integrity test
HMAC DRBG (A3833)	HMAC-SHA2-256, HMAC-SHA2-512, with/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
HMAC DRBG (A3834)	HMAC-SHA2-256, HMAC-SHA2-512, with/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
HMAC DRBG (A3840)	HMAC-SHA2-256, HMAC-SHA2-512, with/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
HMAC DRBG (A3841)	HMAC-SHA2-256, HMAC-SHA2-512, with/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
HMAC DRBG (A3842)	HMAC-SHA2-256, HMAC-SHA2-512, with/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
HMAC DRBG (A3843)	HMAC-SHA2-256, HMAC-SHA2-512, with/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
HMAC DRBG (A3844)	HMAC-SHA2-256, HMAC-SHA2-512, with/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
HMAC DRBG (A3845)	HMAC-SHA2-256, HMAC-SHA2-512, with/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
HMAC DRBG (A3850)	HMAC-SHA2-256, HMAC-SHA2-512, with/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
HMAC DRBG (A3851)	HMAC-SHA2-256, HMAC-SHA2-512, with/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
HMAC DRBG (A3852)	HMAC-SHA2-256, HMAC-SHA2-512, with/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
HMAC DRBG (A3855)	HMAC-SHA2-256, HMAC-SHA2-512, with/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
HMAC DRBG (A3856)	HMAC-SHA2-256, HMAC-SHA2-512, with/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate,	Test runs at power-on

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
					reseed, generate) health test	before the integrity test
KAS-ECC-SSC Sp800-56Ar3 (A3813)	P-256, P-384 curves	KAT	CAST	Module becomes operational	Shared secret computation	Test runs at power-on before the integrity test
KAS-FFC-SSC Sp800-56Ar3 (A3812)	ffdhe2048	PCT	CAST	Module becomes operational	Shared secret computation	Test runs at power-on before the integrity test
RSA SigVer (FIPS186-4) (A3814)	PKCS#1 v1.5 with 2048 bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
RSA SigVer (FIPS186-4) (A3832)	PKCS#1 v1.5 with 2048 bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
RSA SigVer (FIPS186-4) (A3850)	PKCS#1 v1.5 with 2048 bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
RSA SigVer (FIPS186-4) (A3851)	PKCS#1 v1.5 with 2048 bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
RSA SigVer (FIPS186-4) (A3852)	PKCS#1 v1.5 with 2048 bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
Safe Primes Key Generation (A3812)	ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192, Section 5.6.1.1.4 Testing Candidates	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
ECDSA KeyGen (FIPS186-4) (A3813)	SHA2-256, P-256, P-384 curves, Appendix B.4.2 Testing Candidates	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
Entropy Source RCT Startup	1024 samples	RCT	CAST	Module becomes operational and services are available for use	Entropy source startup test	Entropy source initialization
Entropy Source APT Startup	1024 samples	APT	CAST	Module becomes operational and services are available for use	Entropy source startup test	Entropy source initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
Entropy Source RCT Continuous	Intermittent Cutoff: 31 samples, Permanent Cutoff: 61 samples	RCT	CAST	Entropy source is operational	Entropy source continuous test	Continuously
Entropy Source APT Continuous	512 samples, Intermittent Cutoff: 325 samples, Permanent Cutoff: 355 samples	APT	CAST	Entropy source is operational	Entropy source continuous test	Continuously

Table 21: Conditional Self-Tests

If any conditional self-test fails, the module enters the Error State.

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
HMAC-SHA2-256 (A3852) - x86 libkcapi	Message Authentication	SW/FW Integrity	On Demand	Manually
HMAC-SHA2-512 (A3852) - x86 kernel	Message Authentication	SW/FW Integrity	On Demand	Manually
HMAC-SHA2-512 (A3852) - x86 sha512hmac	Message Authentication	SW/FW Integrity	On Demand	Manually
HMAC-SHA2-256 (A3832) - s390 libkcapi	Message Authentication	SW/FW Integrity	On Demand	Manually
HMAC-SHA2-512 (A3832) - s390 kernel	Message Authentication	SW/FW Integrity	On Demand	Manually
HMAC-SHA2-512 (A3832) - s390 sha512hmac	Message Authentication	SW/FW Integrity	On Demand	Manually
HMAC-SHA2-256 (A3858) - arm libkcapi	Message Authentication	SW/FW Integrity	On Demand	Manually
HMAC-SHA2-512 (A3858) - arm kernel	Message Authentication	SW/FW Integrity	On Demand	Manually
HMAC-SHA2-512 (A3858) - arm sha512hmac	Message Authentication	SW/FW Integrity	On Demand	Manually
RSA SigVer (FIPS186-4) (A3852) - x86 .ko files	Signature Verification	SW/FW Integrity	On Demand	Manually
RSA SigVer (FIPS186-4) (A3832) - s390 .ko files	Signature Verification	SW/FW Integrity	On Demand	Manually
RSA SigVer (FIPS186-4) (A3814) - arm .ko files	Signature Verification	SW/FW Integrity	On Demand	Manually

Table 22: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-ECB (A3812) - Encrypt	KAT	CAST	On Demand	Manually
AES-ECB (A3813) - Encrypt	KAT	CAST	On Demand	Manually
AES-ECB (A3814) - Encrypt	KAT	CAST	On Demand	Manually
AES-ECB (A3820) - Encrypt	KAT	CAST	On Demand	Manually
AES-ECB (A3821) - Encrypt	KAT	CAST	On Demand	Manually
AES-ECB (A3822) - Encrypt	KAT	CAST	On Demand	Manually
AES-ECB (A3824) - Encrypt	KAT	CAST	On Demand	Manually
AES-ECB (A3825) - Encrypt	KAT	CAST	On Demand	Manually
AES-ECB (A3829) - Encrypt	KAT	CAST	On Demand	Manually
AES-ECB (A3830) - Encrypt	KAT	CAST	On Demand	Manually
AES-ECB (A3831) - Encrypt	KAT	CAST	On Demand	Manually
AES-ECB (A3832) - Encrypt	KAT	CAST	On Demand	Manually
AES-ECB (A3833) - Encrypt	KAT	CAST	On Demand	Manually
AES-ECB (A3834) - Encrypt	KAT	CAST	On Demand	Manually
AES-ECB (A3840) - Encrypt	KAT	CAST	On Demand	Manually
AES-ECB (A3841) - Encrypt	KAT	CAST	On Demand	Manually
AES-ECB (A3842) - Encrypt	KAT	CAST	On Demand	Manually
AES-ECB (A3843) - Encrypt	KAT	CAST	On Demand	Manually
AES-ECB (A3844) - Encrypt	KAT	CAST	On Demand	Manually
AES-ECB (A3845) - Encrypt	KAT	CAST	On Demand	Manually
AES-ECB (A3853) - Encrypt	KAT	CAST	On Demand	Manually
AES-ECB (A3854) - Encrypt	KAT	CAST	On Demand	Manually
AES-ECB (A3855) - Encrypt	KAT	CAST	On Demand	Manually
AES-ECB (A3856) - Encrypt	KAT	CAST	On Demand	Manually
AES-ECB (A3857) - Encrypt	KAT	CAST	On Demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-CBC (A3814) - Encrypt	KAT	CAST	On Demand	Manually
AES-CBC (A3822) - Encrypt	KAT	CAST	On Demand	Manually
AES-CBC (A3829) - Encrypt	KAT	CAST	On Demand	Manually
AES-CBC (A3832) - Encrypt	KAT	CAST	On Demand	Manually
AES-CBC (A3840) - Encrypt	KAT	CAST	On Demand	Manually
AES-CBC (A3843) - Encrypt	KAT	CAST	On Demand	Manually
AES-CBC (A3853) - Encrypt	KAT	CAST	On Demand	Manually
AES-CBC (A3854) - Encrypt	KAT	CAST	On Demand	Manually
AES-CBC (A3857) - Encrypt	KAT	CAST	On Demand	Manually
AES-CBC-CS3 (A3819) - Encrypt	KAT	CAST	On Demand	Manually
AES-CBC-CS3 (A3828) - Encrypt	KAT	CAST	On Demand	Manually
AES-CBC-CS3 (A3838) - Encrypt	KAT	CAST	On Demand	Manually
AES-CBC-CS3 (A3849) - Encrypt	KAT	CAST	On Demand	Manually
AES-CBC-CS3 (A3853) - Encrypt	KAT	CAST	On Demand	Manually
AES-CBC-CS3 (A3854) - Encrypt	KAT	CAST	On Demand	Manually
AES-CFB128 (A3817) - Encrypt	KAT	CAST	On Demand	Manually
AES-CFB128 (A3826) - Encrypt	KAT	CAST	On Demand	Manually
AES-CFB128 (A3836) - Encrypt	KAT	CAST	On Demand	Manually
AES-CFB128 (A3847) - Encrypt	KAT	CAST	On Demand	Manually
AES-CFB128 (A3854) - Encrypt	KAT	CAST	On Demand	Manually
AES-CTR (A3814) - Encrypt	KAT	CAST	On Demand	Manually
AES-CTR (A3822) - Encrypt	KAT	CAST	On Demand	Manually
AES-CTR (A3829) - Encrypt	KAT	CAST	On Demand	Manually
AES-CTR (A3832) - Encrypt	KAT	CAST	On Demand	Manually
AES-CTR (A3840) - Encrypt	KAT	CAST	On Demand	Manually
AES-CTR (A3843) - Encrypt	KAT	CAST	On Demand	Manually
AES-CTR (A3853) - Encrypt	KAT	CAST	On Demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-CTR (A3854) - Encrypt	KAT	CAST	On Demand	Manually
AES-CTR (A3857) - Encrypt	KAT	CAST	On Demand	Manually
AES-CCM (A3814) - Encrypt	KAT	CAST	On Demand	Manually
AES-CCM (A3822) - Encrypt	KAT	CAST	On Demand	Manually
AES-CCM (A3829) - Encrypt	KAT	CAST	On Demand	Manually
AES-CCM (A3832) - Encrypt	KAT	CAST	On Demand	Manually
AES-CCM (A3843) - Encrypt	KAT	CAST	On Demand	Manually
AES-CCM (A3853) - Encrypt	KAT	CAST	On Demand	Manually
AES-CCM (A3854) - Encrypt	KAT	CAST	On Demand	Manually
AES-GCM (A3814) - Encrypt	KAT	CAST	On Demand	Manually
AES-GCM (A3820) - Encrypt	KAT	CAST	On Demand	Manually
AES-GCM (A3821) - Encrypt	KAT	CAST	On Demand	Manually
AES-GCM (A3822) - Encrypt	KAT	CAST	On Demand	Manually
AES-GCM (A3824) - Encrypt	KAT	CAST	On Demand	Manually
AES-GCM (A3825) - Encrypt	KAT	CAST	On Demand	Manually
AES-GCM (A3829) - Encrypt	KAT	CAST	On Demand	Manually
AES-GCM (A3830) - Encrypt	KAT	CAST	On Demand	Manually
AES-GCM (A3831) - Encrypt	KAT	CAST	On Demand	Manually
AES-GCM (A3832) - Encrypt	KAT	CAST	On Demand	Manually
AES-GCM (A3833) - Encrypt	KAT	CAST	On Demand	Manually
AES-GCM (A3834) - Encrypt	KAT	CAST	On Demand	Manually
AES-GCM (A3840) - Encrypt	KAT	CAST	On Demand	Manually
AES-GCM (A3841) - Encrypt	KAT	CAST	On Demand	Manually
AES-GCM (A3842) - Encrypt	KAT	CAST	On Demand	Manually
AES-GCM (A3843) - Encrypt	KAT	CAST	On Demand	Manually
AES-GCM (A3844) - Encrypt	KAT	CAST	On Demand	Manually
AES-GCM (A3845) - Encrypt	KAT	CAST	On Demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-GCM (A3854) - Encrypt	KAT	CAST	On Demand	Manually
AES-GCM (A3855) - Encrypt	KAT	CAST	On Demand	Manually
AES-GCM (A3856) - Encrypt	KAT	CAST	On Demand	Manually
AES-KW (A3815) - Encrypt	KAT	CAST	On Demand	Manually
AES-KW (A3823) - Encrypt	KAT	CAST	On Demand	Manually
AES-KW (A3835) - Encrypt	KAT	CAST	On Demand	Manually
AES-KW (A3846) - Encrypt	KAT	CAST	On Demand	Manually
AES-OFB (A3818) - Encrypt	KAT	CAST	On Demand	Manually
AES-OFB (A3827) - Encrypt	KAT	CAST	On Demand	Manually
AES-OFB (A3837) - Encrypt	KAT	CAST	On Demand	Manually
AES-OFB (A3848) - Encrypt	KAT	CAST	On Demand	Manually
AES-OFB (A3854) - Encrypt	KAT	CAST	On Demand	Manually
AES-XTS Testing Revision 2.0 (A3814) - Encrypt	KAT	CAST	On Demand	Manually
AES-XTS Testing Revision 2.0 (A3822) - Encrypt	KAT	CAST	On Demand	Manually
AES-XTS Testing Revision 2.0 (A3829) - Encrypt	KAT	CAST	On Demand	Manually
AES-XTS Testing Revision 2.0 (A3832) - Encrypt	KAT	CAST	On Demand	Manually
AES-XTS Testing Revision 2.0 (A3840) - Encrypt	KAT	CAST	On Demand	Manually
AES-XTS Testing Revision 2.0 (A3843) - Encrypt	KAT	CAST	On Demand	Manually
AES-XTS Testing Revision 2.0 (A3853) - Encrypt	KAT	CAST	On Demand	Manually
AES-XTS Testing Revision 2.0 (A3854) - Encrypt	KAT	CAST	On Demand	Manually
AES-XTS Testing Revision 2.0 (A3857) - Encrypt	KAT	CAST	On Demand	Manually
AES-ECB (A3812) - Decrypt	KAT	CAST	On Demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-ECB (A3813) - Decrypt	KAT	CAST	On Demand	Manually
AES-ECB (A3814) - Decrypt	KAT	CAST	On Demand	Manually
AES-ECB (A3820) - Decrypt	KAT	CAST	On Demand	Manually
AES-ECB (A3821) - Decrypt	KAT	CAST	On Demand	Manually
AES-ECB (A3822) - Decrypt	KAT	CAST	On Demand	Manually
AES-ECB (A3824) - Decrypt	KAT	CAST	On Demand	Manually
AES-ECB (A3825) - Decrypt	KAT	CAST	On Demand	Manually
AES-ECB (A3829) - Decrypt	KAT	CAST	On Demand	Manually
AES-ECB (A3830) - Decrypt	KAT	CAST	On Demand	Manually
AES-ECB (A3831) - Decrypt	KAT	CAST	On Demand	Manually
AES-ECB (A3832) - Decrypt	KAT	CAST	On Demand	Manually
AES-ECB (A3833) - Decrypt	KAT	CAST	On Demand	Manually
AES-ECB (A3834) - Decrypt	KAT	CAST	On Demand	Manually
AES-ECB (A3840) - Decrypt	KAT	CAST	On Demand	Manually
AES-ECB (A3841) - Decrypt	KAT	CAST	On Demand	Manually
AES-ECB (A3842) - Decrypt	KAT	CAST	On Demand	Manually
AES-ECB (A3843) - Decrypt	KAT	CAST	On Demand	Manually
AES-ECB (A3844) - Decrypt	KAT	CAST	On Demand	Manually
AES-ECB (A3845) - Decrypt	KAT	CAST	On Demand	Manually
AES-ECB (A3853) - Decrypt	KAT	CAST	On Demand	Manually
AES-ECB (A3854) - Decrypt	KAT	CAST	On Demand	Manually
AES-ECB (A3855) - Decrypt	KAT	CAST	On Demand	Manually
AES-ECB (A3856) - Decrypt	KAT	CAST	On Demand	Manually
AES-ECB (A3857) - Decrypt	KAT	CAST	On Demand	Manually
AES-CBC (A3814) - Decrypt	KAT	CAST	On Demand	Manually
AES-CBC (A3822) - Decrypt	KAT	CAST	On Demand	Manually
AES-CBC (A3829) - Decrypt	KAT	CAST	On Demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-CBC (A3832) - Decrypt	KAT	CAST	On Demand	Manually
AES-CBC (A3840) - Decrypt	KAT	CAST	On Demand	Manually
AES-CBC (A3843) - Decrypt	KAT	CAST	On Demand	Manually
AES-CBC (A3853) - Decrypt	KAT	CAST	On Demand	Manually
AES-CBC (A3854) - Decrypt	KAT	CAST	On Demand	Manually
AES-CBC (A3857) - Decrypt	KAT	CAST	On Demand	Manually
AES-CBC-CS3 (A3819) - Decrypt	KAT	CAST	On Demand	Manually
AES-CBC-CS3 (A3828) - Decrypt	KAT	CAST	On Demand	Manually
AES-CBC-CS3 (A3838) - Decrypt	KAT	CAST	On Demand	Manually
AES-CBC-CS3 (A3849) - Decrypt	KAT	CAST	On Demand	Manually
AES-CBC-CS3 (A3853) - Decrypt	KAT	CAST	On Demand	Manually
AES-CBC-CS3 (A3854) - Decrypt	KAT	CAST	On Demand	Manually
AES-CFB128 (A3817) - Decrypt	KAT	CAST	On Demand	Manually
AES-CFB128 (A3826) - Decrypt	KAT	CAST	On Demand	Manually
AES-CFB128 (A3836) - Decrypt	KAT	CAST	On Demand	Manually
AES-CFB128 (A3847) - Decrypt	KAT	CAST	On Demand	Manually
AES-CFB128 (A3854) - Decrypt	KAT	CAST	On Demand	Manually
AES-CTR (A3814) - Decrypt	KAT	CAST	On Demand	Manually
AES-CTR (A3822) - Decrypt	KAT	CAST	On Demand	Manually
AES-CTR (A3829) - Decrypt	KAT	CAST	On Demand	Manually
AES-CTR (A3832) - Decrypt	KAT	CAST	On Demand	Manually
AES-CTR (A3840) - Decrypt	KAT	CAST	On Demand	Manually
AES-CTR (A3843) - Decrypt	KAT	CAST	On Demand	Manually
AES-CTR (A3853) - Decrypt	KAT	CAST	On Demand	Manually
AES-CTR (A3854) - Decrypt	KAT	CAST	On Demand	Manually
AES-CTR (A3857) - Decrypt	KAT	CAST	On Demand	Manually
AES-CCM (A3814) - Decrypt	KAT	CAST	On Demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-CCM (A3822) - Decrypt	KAT	CAST	On Demand	Manually
AES-CCM (A3829) - Decrypt	KAT	CAST	On Demand	Manually
AES-CCM (A3832) - Decrypt	KAT	CAST	On Demand	Manually
AES-CCM (A3843) - Decrypt	KAT	CAST	On Demand	Manually
AES-CCM (A3853) - Decrypt	KAT	CAST	On Demand	Manually
AES-CCM (A3854) - Decrypt	KAT	CAST	On Demand	Manually
AES-GCM (A3814) - Decrypt	KAT	CAST	On Demand	Manually
AES-GCM (A3820) - Decrypt	KAT	CAST	On Demand	Manually
AES-GCM (A3821) - Decrypt	KAT	CAST	On Demand	Manually
AES-GCM (A3822) - Decrypt	KAT	CAST	On Demand	Manually
AES-GCM (A3824) - Decrypt	KAT	CAST	On Demand	Manually
AES-GCM (A3825) - Decrypt	KAT	CAST	On Demand	Manually
AES-GCM (A3829) - Decrypt	KAT	CAST	On Demand	Manually
AES-GCM (A3830) - Decrypt	KAT	CAST	On Demand	Manually
AES-GCM (A3831) - Decrypt	KAT	CAST	On Demand	Manually
AES-GCM (A3832) - Decrypt	KAT	CAST	On Demand	Manually
AES-GCM (A3833) - Decrypt	KAT	CAST	On Demand	Manually
AES-GCM (A3834) - Decrypt	KAT	CAST	On Demand	Manually
AES-GCM (A3840) - Decrypt	KAT	CAST	On Demand	Manually
AES-GCM (A3841) - Decrypt	KAT	CAST	On Demand	Manually
AES-GCM (A3842) - Decrypt	KAT	CAST	On Demand	Manually
AES-GCM (A3843) - Decrypt	KAT	CAST	On Demand	Manually
AES-GCM (A3844) - Decrypt	KAT	CAST	On Demand	Manually
AES-GCM (A3845) - Decrypt	KAT	CAST	On Demand	Manually
AES-GCM (A3854) - Decrypt	KAT	CAST	On Demand	Manually
AES-GCM (A3855) - Decrypt	KAT	CAST	On Demand	Manually
AES-GCM (A3856) - Decrypt	KAT	CAST	On Demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-KW (A3815) - Decrypt	KAT	CAST	On Demand	Manually
AES-KW (A3823) - Decrypt	KAT	CAST	On Demand	Manually
AES-KW (A3835) - Decrypt	KAT	CAST	On Demand	Manually
AES-KW (A3846) - Decrypt	KAT	CAST	On Demand	Manually
AES-OFB (A3818) - Decrypt	KAT	CAST	On Demand	Manually
AES-OFB (A3827) - Decrypt	KAT	CAST	On Demand	Manually
AES-OFB (A3837) - Decrypt	KAT	CAST	On Demand	Manually
AES-OFB (A3848) - Decrypt	KAT	CAST	On Demand	Manually
AES-OFB (A3854) - Decrypt	KAT	CAST	On Demand	Manually
AES-XTS Testing Revision 2.0 (A3814) - Decrypt	KAT	CAST	On Demand	Manually
AES-XTS Testing Revision 2.0 (A3822) - Decrypt	KAT	CAST	On Demand	Manually
AES-XTS Testing Revision 2.0 (A3829) - Decrypt	KAT	CAST	On Demand	Manually
AES-XTS Testing Revision 2.0 (A3832) - Decrypt	KAT	CAST	On Demand	Manually
AES-XTS Testing Revision 2.0 (A3840) - Decrypt	KAT	CAST	On Demand	Manually
AES-XTS Testing Revision 2.0 (A3843) - Decrypt	KAT	CAST	On Demand	Manually
AES-XTS Testing Revision 2.0 (A3853) - Decrypt	KAT	CAST	On Demand	Manually
AES-XTS Testing Revision 2.0 (A3854) - Decrypt	KAT	CAST	On Demand	Manually
AES-XTS Testing Revision 2.0 (A3857) - Decrypt	KAT	CAST	On Demand	Manually
AES-CMAC (A3814)	KAT	CAST	On Demand	Manually
AES-CMAC (A3822)	KAT	CAST	On Demand	Manually
AES-CMAC (A3829)	KAT	CAST	On Demand	Manually
AES-CMAC (A3832)	KAT	CAST	On Demand	Manually
AES-CMAC (A3843)	KAT	CAST	On Demand	Manually
AES-CMAC (A3853)	KAT	CAST	On Demand	Manually
AES-CMAC (A3854)	KAT	CAST	On Demand	Manually
SHA-1 (A3812)	KAT	CAST	On Demand	Manually
SHA-1 (A3813)	KAT	CAST	On Demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
SHA-1 (A3814)	KAT	CAST	On Demand	Manually
SHA-1 (A3832)	KAT	CAST	On Demand	Manually
SHA-1 (A3850)	KAT	CAST	On Demand	Manually
SHA-1 (A3851)	KAT	CAST	On Demand	Manually
SHA-1 (A3852)	KAT	CAST	On Demand	Manually
SHA-1 (A3853)	KAT	CAST	On Demand	Manually
SHA2-224 (A3812)	KAT	CAST	On Demand	Manually
SHA2-224 (A3813)	KAT	CAST	On Demand	Manually
SHA2-224 (A3814)	KAT	CAST	On Demand	Manually
SHA2-224 (A3832)	KAT	CAST	On Demand	Manually
SHA2-224 (A3850)	KAT	CAST	On Demand	Manually
SHA2-224 (A3851)	KAT	CAST	On Demand	Manually
SHA2-224 (A3852)	KAT	CAST	On Demand	Manually
SHA2-224 (A3853)	KAT	CAST	On Demand	Manually
SHA2-224 (A3857)	KAT	CAST	On Demand	Manually
SHA2-224 (A3858)	KAT	CAST	On Demand	Manually
SHA2-256 (A3812)	KAT	CAST	On Demand	Manually
SHA2-256 (A3813)	KAT	CAST	On Demand	Manually
SHA2-256 (A3814)	KAT	CAST	On Demand	Manually
SHA2-256 (A3832)	KAT	CAST	On Demand	Manually
SHA2-256 (A3850)	KAT	CAST	On Demand	Manually
SHA2-256 (A3851)	KAT	CAST	On Demand	Manually
SHA2-256 (A3852)	KAT	CAST	On Demand	Manually
SHA2-256 (A3853)	KAT	CAST	On Demand	Manually
SHA2-256 (A3857)	KAT	CAST	On Demand	Manually
SHA2-256 (A3858)	KAT	CAST	On Demand	Manually
SHA2-384 (A3812)	KAT	CAST	On Demand	Manually
SHA2-384 (A3813)	KAT	CAST	On Demand	Manually
SHA2-384 (A3814)	KAT	CAST	On Demand	Manually
SHA2-384 (A3832)	KAT	CAST	On Demand	Manually
SHA2-384 (A3850)	KAT	CAST	On Demand	Manually
SHA2-384 (A3851)	KAT	CAST	On Demand	Manually
SHA2-384 (A3852)	KAT	CAST	On Demand	Manually
SHA2-384 (A3858)	KAT	CAST	On Demand	Manually
SHA2-512 (A3812)	KAT	CAST	On Demand	Manually
SHA2-512 (A3813)	KAT	CAST	On Demand	Manually
SHA2-512 (A3814)	KAT	CAST	On Demand	Manually
SHA2-512 (A3832)	KAT	CAST	On Demand	Manually
SHA2-512 (A3850)	KAT	CAST	On Demand	Manually
SHA2-512 (A3851)	KAT	CAST	On Demand	Manually
SHA2-512 (A3852)	KAT	CAST	On Demand	Manually
SHA2-512 (A3858)	KAT	CAST	On Demand	Manually
SHA3-224 (A3816)	KAT	CAST	On Demand	Manually
SHA3-224 (A3839)	KAT	CAST	On Demand	Manually
SHA3-256 (A3816)	KAT	CAST	On Demand	Manually
SHA3-256 (A3839)	KAT	CAST	On Demand	Manually
SHA3-384 (A3816)	KAT	CAST	On Demand	Manually
SHA3-384 (A3839)	KAT	CAST	On Demand	Manually
SHA3-512 (A3816)	KAT	CAST	On Demand	Manually
SHA3-512 (A3839)	KAT	CAST	On Demand	Manually
HMAC-SHA-1 (A3812)	KAT	CAST	On Demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
HMAC-SHA-1 (A3813)	KAT	CAST	On Demand	Manually
HMAC-SHA-1 (A3814)	KAT	CAST	On Demand	Manually
HMAC-SHA-1 (A3832)	KAT	CAST	On Demand	Manually
HMAC-SHA-1 (A3850)	KAT	CAST	On Demand	Manually
HMAC-SHA-1 (A3851)	KAT	CAST	On Demand	Manually
HMAC-SHA-1 (A3852)	KAT	CAST	On Demand	Manually
HMAC-SHA-1 (A3853)	KAT	CAST	On Demand	Manually
HMAC-SHA2-224 (A3812)	KAT	CAST	On Demand	Manually
HMAC-SHA2-224 (A3813)	KAT	CAST	On Demand	Manually
HMAC-SHA2-224 (A3814)	KAT	CAST	On Demand	Manually
HMAC-SHA2-224 (A3832)	KAT	CAST	On Demand	Manually
HMAC-SHA2-224 (A3850)	KAT	CAST	On Demand	Manually
HMAC-SHA2-224 (A3851)	KAT	CAST	On Demand	Manually
HMAC-SHA2-224 (A3852)	KAT	CAST	On Demand	Manually
HMAC-SHA2-224 (A3853)	KAT	CAST	On Demand	Manually
HMAC-SHA2-224 (A3857)	KAT	CAST	On Demand	Manually
HMAC-SHA2-224 (A3858)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A3812)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A3813)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A3814)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A3832)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A3850)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A3851)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A3852)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A3853)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A3857)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A3858)	KAT	CAST	On Demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
HMAC-SHA2-384 (A3812)	KAT	CAST	On Demand	Manually
HMAC-SHA2-384 (A3813)	KAT	CAST	On Demand	Manually
HMAC-SHA2-384 (A3814)	KAT	CAST	On Demand	Manually
HMAC-SHA2-384 (A3832)	KAT	CAST	On Demand	Manually
HMAC-SHA2-384 (A3850)	KAT	CAST	On Demand	Manually
HMAC-SHA2-384 (A3851)	KAT	CAST	On Demand	Manually
HMAC-SHA2-384 (A3852)	KAT	CAST	On Demand	Manually
HMAC-SHA2-384 (A3858)	KAT	CAST	On Demand	Manually
HMAC-SHA2-512 (A3812)	KAT	CAST	On Demand	Manually
HMAC-SHA2-512 (A3813)	KAT	CAST	On Demand	Manually
HMAC-SHA2-512 (A3814)	KAT	CAST	On Demand	Manually
HMAC-SHA2-512 (A3832)	KAT	CAST	On Demand	Manually
HMAC-SHA2-512 (A3850)	KAT	CAST	On Demand	Manually
HMAC-SHA2-512 (A3851)	KAT	CAST	On Demand	Manually
HMAC-SHA2-512 (A3852)	KAT	CAST	On Demand	Manually
HMAC-SHA2-512 (A3858)	KAT	CAST	On Demand	Manually
HMAC-SHA3-224 (A3816)	KAT	CAST	On Demand	Manually
HMAC-SHA3-224 (A3839)	KAT	CAST	On Demand	Manually
HMAC-SHA3-256 (A3816)	KAT	CAST	On Demand	Manually
HMAC-SHA3-256 (A3839)	KAT	CAST	On Demand	Manually
HMAC-SHA3-384 (A3816)	KAT	CAST	On Demand	Manually
HMAC-SHA3-384 (A3839)	KAT	CAST	On Demand	Manually
HMAC-SHA3-512 (A3816)	KAT	CAST	On Demand	Manually
HMAC-SHA3-512 (A3839)	KAT	CAST	On Demand	Manually
Counter DRBG (A3812)	KAT	CAST	On Demand	Manually
Counter DRBG (A3813)	KAT	CAST	On Demand	Manually
Counter DRBG (A3814)	KAT	CAST	On Demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
Counter DRBG (A3820)	KAT	CAST	On Demand	Manually
Counter DRBG (A3821)	KAT	CAST	On Demand	Manually
Counter DRBG (A3822)	KAT	CAST	On Demand	Manually
Counter DRBG (A3824)	KAT	CAST	On Demand	Manually
Counter DRBG (A3825)	KAT	CAST	On Demand	Manually
Counter DRBG (A3829)	KAT	CAST	On Demand	Manually
Counter DRBG (A3830)	KAT	CAST	On Demand	Manually
Counter DRBG (A3831)	KAT	CAST	On Demand	Manually
Counter DRBG (A3832)	KAT	CAST	On Demand	Manually
Counter DRBG (A3833)	KAT	CAST	On Demand	Manually
Counter DRBG (A3834)	KAT	CAST	On Demand	Manually
Counter DRBG (A3840)	KAT	CAST	On Demand	Manually
Counter DRBG (A3841)	KAT	CAST	On Demand	Manually
Counter DRBG (A3842)	KAT	CAST	On Demand	Manually
Counter DRBG (A3843)	KAT	CAST	On Demand	Manually
Counter DRBG (A3844)	KAT	CAST	On Demand	Manually
Counter DRBG (A3845)	KAT	CAST	On Demand	Manually
Counter DRBG (A3854)	KAT	CAST	On Demand	Manually
Counter DRBG (A3855)	KAT	CAST	On Demand	Manually
Counter DRBG (A3856)	KAT	CAST	On Demand	Manually
Hash DRBG (A3812)	KAT	CAST	On Demand	Manually
Hash DRBG (A3813)	KAT	CAST	On Demand	Manually
Hash DRBG (A3814)	KAT	CAST	On Demand	Manually
Hash DRBG (A3820)	KAT	CAST	On Demand	Manually
Hash DRBG (A3821)	KAT	CAST	On Demand	Manually
Hash DRBG (A3822)	KAT	CAST	On Demand	Manually
Hash DRBG (A3824)	KAT	CAST	On Demand	Manually
Hash DRBG (A3825)	KAT	CAST	On Demand	Manually
Hash DRBG (A3830)	KAT	CAST	On Demand	Manually
Hash DRBG (A3831)	KAT	CAST	On Demand	Manually
Hash DRBG (A3832)	KAT	CAST	On Demand	Manually
Hash DRBG (A3833)	KAT	CAST	On Demand	Manually
Hash DRBG (A3834)	KAT	CAST	On Demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
Hash DRBG (A3840)	KAT	CAST	On Demand	Manually
Hash DRBG (A3841)	KAT	CAST	On Demand	Manually
Hash DRBG (A3842)	KAT	CAST	On Demand	Manually
Hash DRBG (A3843)	KAT	CAST	On Demand	Manually
Hash DRBG (A3844)	KAT	CAST	On Demand	Manually
Hash DRBG (A3845)	KAT	CAST	On Demand	Manually
Hash DRBG (A3850)	KAT	CAST	On Demand	Manually
Hash DRBG (A3851)	KAT	CAST	On Demand	Manually
Hash DRBG (A3852)	KAT	CAST	On Demand	Manually
Hash DRBG (A3855)	KAT	CAST	On Demand	Manually
Hash DRBG (A3856)	KAT	CAST	On Demand	Manually
HMAC DRBG (A3812)	KAT	CAST	On Demand	Manually
HMAC DRBG (A3813)	KAT	CAST	On Demand	Manually
HMAC DRBG (A3814)	KAT	CAST	On Demand	Manually
HMAC DRBG (A3820)	KAT	CAST	On Demand	Manually
HMAC DRBG (A3821)	KAT	CAST	On Demand	Manually
HMAC DRBG (A3822)	KAT	CAST	On Demand	Manually
HMAC DRBG (A3824)	KAT	CAST	On Demand	Manually
HMAC DRBG (A3825)	KAT	CAST	On Demand	Manually
HMAC DRBG (A3830)	KAT	CAST	On Demand	Manually
HMAC DRBG (A3831)	KAT	CAST	On Demand	Manually
HMAC DRBG (A3832)	KAT	CAST	On Demand	Manually
HMAC DRBG (A3833)	KAT	CAST	On Demand	Manually
HMAC DRBG (A3834)	KAT	CAST	On Demand	Manually
HMAC DRBG (A3840)	KAT	CAST	On Demand	Manually
HMAC DRBG (A3841)	KAT	CAST	On Demand	Manually
HMAC DRBG (A3842)	KAT	CAST	On Demand	Manually
HMAC DRBG (A3843)	KAT	CAST	On Demand	Manually
HMAC DRBG (A3844)	KAT	CAST	On Demand	Manually
HMAC DRBG (A3845)	KAT	CAST	On Demand	Manually
HMAC DRBG (A3850)	KAT	CAST	On Demand	Manually
HMAC DRBG (A3851)	KAT	CAST	On Demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
HMAC DRBG (A3852)	KAT	CAST	On Demand	Manually
HMAC DRBG (A3855)	KAT	CAST	On Demand	Manually
HMAC DRBG (A3856)	KAT	CAST	On Demand	Manually
KAS-ECC-SSC Sp800-56Ar3 (A3813)	KAT	CAST	On Demand	Manually
KAS-FFC-SSC Sp800-56Ar3 (A3812)	PCT	CAST	On Demand	Manually
RSA SigVer (FIPS186-4) (A3814)	KAT	CAST	On Demand	Manually
RSA SigVer (FIPS186-4) (A3832)	KAT	CAST	On Demand	Manually
RSA SigVer (FIPS186-4) (A3850)	KAT	CAST	On Demand	Manually
RSA SigVer (FIPS186-4) (A3851)	KAT	CAST	On Demand	Manually
RSA SigVer (FIPS186-4) (A3852)	KAT	CAST	On Demand	Manually
Safe Primes Key Generation (A3812)	PCT	PCT	On Demand	Manually
ECDSA KeyGen (FIPS186-4) (A3813)	PCT	PCT	On Demand	Manually
Entropy Source RCT Startup	RCT	CAST	On Demand	Manually
Entropy Source APT Startup	APT	CAST	On Demand	Manually
Entropy Source RCT Continuous	RCT	CAST	On Demand	Manually
Entropy Source APT Continuous	APT	CAST	On Demand	Manually

Table 23: Conditional Periodic Information

10.4 Error States

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

Table 24: Error States

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

10.5 Operator Initiation of Self-Tests

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

The pair-wise consistency tests can be invoked on demand by requesting the key pair generation service.

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

On the Ubuntu 22.04 LTS operational environments, the module is distributed in the form of the following deb packages:

- linux-image-5.15.0-73-fips=5.15.0-73.80+fips1
- linux-modules-5.15.0-73-fips=5.15.0-73.80+fips1
- linux-image-hmac-5.15.0-73-fips=5.15.0-73.80+fips1
- libkcapi1=1.4.0-1ubuntu0.1~Fips1
- kcapi-tools=1.4.0-1ubuntu0.1~Fips1

On the Ubuntu Core 22 operational environments, the module is distributed in the form of the "fips-kernel" snap, with snap-id ZjfoRia9mZzIe2xoWtGxHNUQsSSqjzUK. Revision 4 and 9 are respectively validated for x86 and arm64 platforms.

Once the Ubuntu 22.04 LTS operational environment is configured following the instructions provided in Section 11.1, and configuration to access the PPA is complete, the Crypto Officer can install the Ubuntu packages containing the module using the Advanced Package Tool (APT) with the following command line:

$ sudo apt-get install linux-image-5.15.0-73-fips=5.15.0-73.80+fips1 linux-modules-5.15.0-73-fips=5.15.0-73.80+fips1 linux-image-hmac-5.15.0-73-fips=5.15.0-73.80+fips1 libkcapi1=1.4.0-1ubuntu0.1~Fips1 kcapi-tools=1.4.0-1ubuntu0.1~Fips1

All the Ubuntu packages are associated with hashes for integrity check. The integrity of the Ubuntu package is automatically verified by the packing tool during the installation of the module. The Crypto Officer shall not install the package if the integrity check fails.

Installation of the module on the Ubuntu Core 22 operational environment simply consists of flashing the operating system image to a hard drive, then following the instructions on the screen.

After the module is installed, the Crypto Officer must execute:

$ cat /proc/sys/crypto/fips_name

The Crypto Officer must ensure that the proper name is listed in the output as follows:

Ubuntu 22.04 Kernel Crypto API Cryptographic Module

Then, the Crypto Officer must execute:

$ cat /proc/sys/crypto/fips_version

This command must output the following:

5.15.0-73-fips

On the Ubuntu 22.04 LTS operational environments, versions of the installed packages can be verified using the following command:

$ dpkg-query -W linux-image-5.15.0-73-fips linux-modules-5.15.0-73-fips linux-image-hmac-5.15.0-73-fips libkcapi1 kcapi-tools

On the Ubuntu Core 22 operational environments, revisions of the installed snaps can be verified using the following command:

$ snap list fips-kernel

11.2 Administrator Guidance

The Approved and non-Approved modes of operation are specified in section 2.4. The administrative functions are specified in the *Approved Services* table. All the physical ports and logical interfaces are specified in section 3.1.

11.3 Non-Administrator Guidance

The approved and non-approved security functions available to users are listed in section 2, the physical ports, and logical interfaces available to users are specified in section 3.1. The Approved and non-Approved modes of operation are specified in section 2.4. The algorithm-specific information is listed in section 2.7.

11.4 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.

If desired, the linux-image-5.15.0-73-fips, linux-modules-5.15.0-73-fips, linux-image-hmac-5.15.0-73-fips, libkcapi1, and kcapi-tools deb packages can be uninstalled from the Ubuntu 22.04 LTS system.

The Ubuntu Core 22 system is distributed as an operating system image, so removing this image will also uninstall the module. Alternatively, the “snap remodel” command can be used to switch to a generic model with a different kernel.

12 Mitigation of Other Attacks

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

Appendix A. Glossary and Abbreviations

AES	Advanced Encryption Standard
API	Application Programming Interface
CAST	Cryptographic Algorithm Self-Test
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher Block Chaining
CCM	Counter with Cipher Block Chaining-Message Authentication Code
CFB	Cipher Feedback
CKG	Cryptographic Key Generation
CMAC	Cipher-based Message Authentication Code
CMVP	Cryptographic Module Validation Program
CSP	Critical Security Parameter
CTR	Counter
CTS	Ciphertext Stealing
DRBG	Deterministic Random Bit Generator
ECB	Electronic Code Book
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
FFC	Finite Field Cryptography
FIPS	Federal Information Processing Standards
GCM	Galois Counter Mode
GMAC	Galois Counter Mode Message Authentication Code
HKDF	HMAC-based Key Derivation Function
HMAC	Keyed-Hash Message Authentication Code
IPsec	Internet Protocol Security
KAS	Key Agreement Scheme
KAT	Known Answer Test
KBKDF	Key-based Key Derivation Function
KW	Key Wrap
MAC	Message Authentication Code
NIST	National Institute of Science and Technology
OFB	Output Feedback
PAA	Processor Algorithm Acceleration
PAI	Processor Algorithm Implementation
PCT	Pair-wise Consistency Test
PBKDF2	Password-based Key Derivation Function v2
PKCS	Public-Key Cryptography Standards
RSA	Rivest, Shamir, Addleman
SHA	Secure Hash Algorithm
SSC	Shared Secret Computation
SSP	Sensitive Security Parameter
XTS	XEX-based Tweaked-codebook mode with cipher text Stealing

Appendix B. References

FIPS 140-3	**FIPS PUB 140-3 - Security Requirements For Cryptographic Modules** 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 [10-23-2024]** 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 186-4	**Digital Signature Standard (DSS)** July 2013 https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf
FIPS 186-5	**Digital Signature Standard (DSS)** February 2023 https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-5.pdf
FIPS 197	**Advanced Encryption Standard** November 2001 https://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
FIPS 198-1	**The Keyed Hash Message Authentication Code (HMAC)** July 2008 https://csrc.nist.gov/publications/fips/fips198-1/FIPS-198-1_final.pdf
FIPS 202	**SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions** August 2015 https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf
PKCS#1	**Public Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1** February 2003 https://www.ietf.org/rfc/rfc3447.txt
RFC 3526	**More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)** May 2003 https://www.ietf.org/rfc/rfc3526.txt
RFC 4106	**The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)** June 2005 https://datatracker.ietf.org/doc/html/rfc4106
RFC 7296	**Internet Key Exchange Protocol Version 2 (IKEv2)** October 2014 https://datatracker.ietf.org/doc/html/rfc7296

SP 800-38A	**Recommendation for Block Cipher Modes of Operation Methods and Techniques** December 2001 https://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf
SP 800-38A Addendum	**Recommendation for Block Cipher Modes of Operation: Three Variants of Ciphertext Stealing for CBC Mode** October 2010 https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38a-add.pdf
SP 800-38B	**Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication** May 2005 https://csrc.nist.gov/publications/nistpubs/800-38B/SP_800-38B.pdf
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 800-38F	**Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping** December 2012 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-38F.pdf
SP 800-56Ar3	**Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography** April 2018 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Ar3.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
SP 800-90B	**Recommendation for the Entropy Sources Used for Random Bit Generation** January 2018 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90B.pdf

SP 800-133r2 **Recommendation for Cryptographic Key Generation**
June 2020
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-133r2.pdf

SP 800-140Br1 **CMVP Security Policy Requirements**
March 2020
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-140Br1.pdf