SUSE LLC

SUSE Linux Enterprise Kernel Crypto API Cryptographic Module

FIPS 140-3 Non-Proprietary Security Policy

Prepared by:

atsec information security corporation
4516 Seton Center Pkwy, Suite 250
Austin, TX 78759
www.atsec.com

Document version: 1.1
Last update: 12-04-2025

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 versions 3.5 and 3.6 the SUSE Linux Enterprise 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.

1.1.1 How this Security Policy was prepared

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

1.2 Security Levels

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

Table 1: Security Levels

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:
The SUSE Linux Enterprise 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: MultiChipStand

Cryptographic Boundary:
The cryptographic boundary of the module is defined as the kernel binary and the kernel crypto object files, the libkcapi library, and the fipscheck 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. It includes software in kernel and user space, as well as the PAA in the CPU. The TOEPP is indicated by the large thin border in Figure 1.

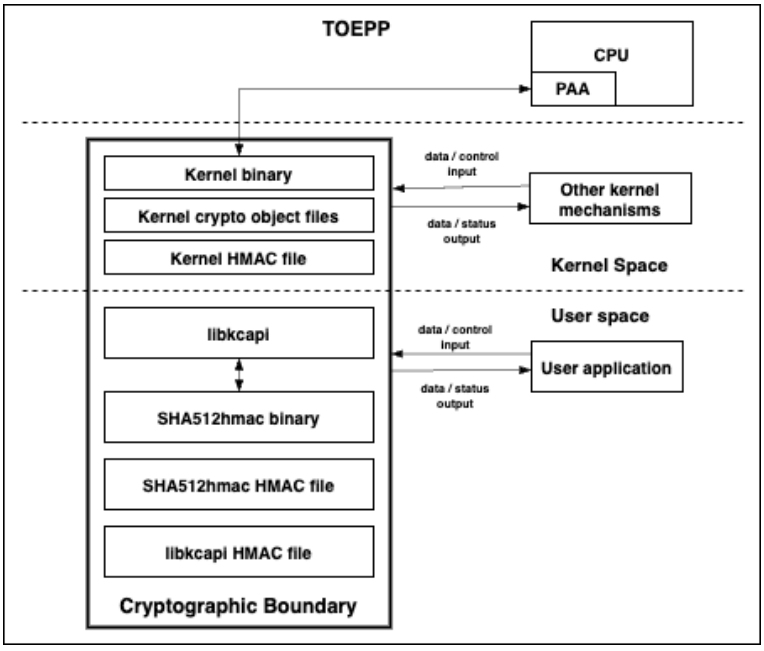

Figure 1: Block Diagram

2.2 Tested and Vendor Affirmed Module Version and Identification

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

Package or File Name	Software/ Firmware Version	Features	Integrity Test
For AMD and Intel Xeon platforms: /boot/vmlinuz-6.4.0-150600.23.25-default; /boot/.vmlinuz-6.4.0-150600.23.25-default.hmac; /lib/modules/6.4.0-150600.23.25-default/kernel/crypto/*.ko; /lib/modules/6.4.0-150600.23.25-default/kernel/arch/x86/crypto/*.ko; /usr/lib64/libkcapi.so.0.13.0; /usr/lib64/libkcapi/fipscheck; /usr/lib64/libkcapi/.fipscheck.hmac	3.5	N/A	HMAC-SHA2-256; RSA signature verification with SHA2-256 and 4096-bit key
For ARM Ampere Altra platform: /boot/Image-6.4.0-150600.23.25-default; /boot/.Image-6.4.0-150600.23.25-default.hmac; /lib/modules/6.4.0-150600.23.25-default/kernel/crypto/*.ko; /lib/modules/6.4.0-150600.23.25-default/kernel/arch/arm64/crypto/*.ko; /usr/lib64/libkcapi.so.0.13.0; /usr/lib64/libkcapi/fipscheck; /usr/lib64/libkcapi/.fipscheck.hmac	3.5	N/A	HMAC-SHA2-256; RSA signature verification with SHA2-256 and 4096-bit key
For IBM z/16 platform: /boot/image-6.4.0-150600.23.25-default; /boot/.image-6.4.0-150600.23.25-default.hmac; /lib/modules/6.4.0-150600.23.25-default/kernel/crypto/*.ko; /lib/modules/6.4.0-150600.23.25-default/kernel/arch/s390/crypto/*.ko; /usr/lib64/libkcapi.so.0.13.0; /usr/lib64/libkcapi/fipscheck; /usr/lib64/libkcapi/.fipscheck.hmac	3.5	N/A	HMAC-SHA2-256; RSA signature verification with SHA2-256 and 4096-bit key
For AMD and Intel Xeon platforms: /boot/vmlinuz-6.4.0-150600.10.17-rt; /boot/.vmlinuz-6.4.0-150600.10.17-rt.hmac; /lib/modules/6.4.0-150600.10.17-rt/kernel/crypto/*.ko; /lib/modules/6.4.0-150600.10.17-	3.6	N/A	HMAC-SHA2-256; RSA signature verification with SHA2-256

Package or File Name	Software/ Firmware Version	Features	Integrity Test
rt/kernel/arch/x86/crypto/*.ko; /usr/lib64/libkcapi.so.0.13.0; /usr/lib64/libkcapi/fipscheck; /usr/lib64/libkcapi/.fipscheck.hmac			and 4096-bit key

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

Tested Operational Environments - Software, Firmware, Hybrid:

Operating System	Hardware Platform	Processors	PAA/PAI	Hypervisor or Host OS	Version(s)
SUSE Linux Enterprise Server 15 SP6	SuperMicro SuperChassis 825BTQC-R1K23LPB and Motherboard H12DSi-NT6	AMD EPYC(TM) 7343	Yes	N/A	3.5 3.6
SUSE Linux Enterprise Server 15 SP6	SuperMicro SuperChassis 825BTQC-R1K23LPB and Motherboard H12DSi-NT6	AMD EPYC(TM) 7343	No	N/A	3.5 3.6
SUSE Linux Enterprise Server 15 SP6	GIGABYTE R152-P30	Ampere® Altra® Q80-30	Yes	N/A	3.5
SUSE Linux Enterprise Server 15 SP6	GIGABYTE R152-P30	Ampere® Altra® Q80-30	No	N/A	3.5
SUSE Linux Enterprise Server 15 SP6	IBM z16 A01	IBM® Telum(TM)	Yes	N/A	3.5
SUSE Linux Enterprise Server 15 SP6	IBM z16 A01	IBM® Telum(TM)	No	N/A	3.5

Operating System	Hardware Platform	Processors	PAA/PAI	Hypervisor or Host OS	Version(s)
SUSE Linux Enterprise Server 15 SP6	ASUS RS700-E11-RS4U	Intel® Xeon® Gold 5416S	Yes	N/A	3.5 3.6
SUSE Linux Enterprise Server 15 SP6	ASUS RS700-E11-RS4U	Intel® Xeon® Gold 5416S	No	N/A	3.5 3.6

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

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

Operating System	Hardware Platform
SUSE Linux Enterprise Server for SAP 15SP6	ASUS RS700-E11-RS4U on Intel® Xeon® Gold 5416S
SUSE Linux Enterprise Desktop 15SP6	ASUS RS700-E11-RS4U on Intel® Xeon® Gold 5416S
SUSE Linux Enterprise Server 15SP6	DELL PowerEdge R640 on Intel® Xeon® Gold 6234
SUSE Linux Enterprise Server for SAP 15SP6	SuperMicro SuperChassis 825BTQCR1K23LPB and Motherboard H12DSi-NT6 on AMD EPYC(TM) 7343
SUSE Linux Enterprise Desktop 15SP6	SuperMicro SuperChassis 825BTQCR1K23LPB and Motherboard H12DSi-NT6 on AMD EPYC(TM) 7343
SUSE Linux Enterprise Server 15SP6	IBM LinuxONE III Model LT1 QEMU VM on z15
SUSE Linux Enterprise Server 15SP6	IBM LinuxONE III Model LT1 on z15
SUSE Linux Enterprise Server for SAP 15SP6	QEMU VM on AMD EPYC(TM) 7543P
SUSE Linux Enterprise Server for SAP 15SP6	QEMU VM on Intel® Xeon® Gold 5218R
SUSE Linux Enterprise Desktop 15SP6	QEMU VM on AMD EPYC(TM) 7543P
SUSE Linux Enterprise Desktop 15SP6	QEMU VM on Intel® i7-1195G7

Operating System	Hardware Platform
SUSE Linux Enterprise Server 15SP6	QEMU VM on Intel® Xeon® Gold 6338
SUSE Linux Enterprise Server 15SP6	QEMU VM on Ampere® Altra® Q80-30
SUSE Linux Enterprise Server Real Time 15SP6	ASUS RS700-E11-RS4U on Intel® Xeon® Gold 5416S
SUSE Linux Enterprise Server Real Time 15SP6	SuperMicro SuperChassis 825BTQCR1K23LPB and Motherboard H12DSi-NT6 on AMD EPYC(TM) 7343
SUSE Linux Enterprise Server Real Time 15SP6	QEMU VM on AMD EPYC(TM) 7773X

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

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

The module is considered to maintain compliance with the FIPS 140-3 validation for SUSE products when operating on any general-purpose platform/processor that supports the SUSE Linux Enterprise Server operating system per the vendor affirmation from SUSE based on the allowance FIPS 140-3 management manual [FIPS140-3_MM] section 7.9.1 bullet 1 a i).

2.3 Excluded Components

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

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Type	Status Indicator
Approved mode	Automatically entered whenever an approved service is requested	Approved	Mapped to approved service indicator in Section 4.3 for all approved algorithms except GCM: respective approved service function returns indicator 0. For GCM: crypto_aead_get_flags(tfm) has the CRYPTO_TFM_FIPS_COMPLIANCE flag set
Non-approved mode	Automatically entered whenever a non-approved service is requested	Non-Approved	No service indicator required for non-approved services per IG 2.4.C

Table 5: Modes List and Description

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

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

2.5 Algorithms

Approved Algorithms:

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	A5503, A5507, A5510, A5513, A5520, A5521, A5524, A5526, A5530, A5533, A5536, A5661, A5664	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CBC-CS3	A5503, A5507, A5510, A5513, A5520, A5521, A5526, A5530, A5533, A5536, A5664	Direction - decrypt, encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CCM	A5503, A5507, A5513, A5520, A5521, A5526, A5530, A5536, A5661, A5664	Key Length - 128, 192, 256	SP 800-38C
AES-CFB128	A5503, A5507, A5513, A5521, A5526, A5530, A5536, A5664	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CMAC	A5503, A5507, A5513, A5520, A5521, A5526, A5530, A5536, A5661, A5664	Direction - Generation, Verification Key Length - 128, 192, 256	SP 800-38B
AES-CTR	A5503, A5507, A5510, A5513, A5520, A5521, A5524, A5526, A5530, A5533, A5536, A5661, A5664	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-ECB	A5503, A5505, A5506, A5507, A5508, A5509, A5510, A5511, A5512, A5513, A5514, A5515, A5520, A5521, A5522, A5523, A5524, A5526, A5528, A5529, A5530, A5531, A5532, A5533, A5534, A5535, A5536, A5537,	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A

Algorithm	CAVP Cert	Properties	Reference
	A5538, A5661, A5662, A5663, A5664, A5665, A5666		
AES-GCM	A5503, A5506, A5507, A5509, A5510, A5512, A5513, A5515, A5521, A5523, A5526, A5529, A5530, A5532, A5533, A5535, A5536, A5538, A5661, A5663, A5664, A5666	Direction - Decrypt, Encrypt IV Generation - External Key Length - 128, 192, 256	SP 800-38D
AES-GCM	A5505, A5508, A5511, A5514, A5522, A5528, A5531, A5534, A5537, A5662, A5665	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.2 Key Length - 128, 192, 256	SP 800-38D
AES-GMAC	A5503, A5507, A5513, A5521, A5526, A5530, A5536, A5661, A5664	Direction - Decrypt, Encrypt IV Generation - External Key Length - 128, 192, 256	SP 800-38D
AES-KW	A5503, A5507, A5513, A5521, A5526, A5530, A5536, A5664	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38F
AES-OFB	A5503, A5507, A5513, A5521, A5526, A5530, A5536, A5664	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-XTS Testing Revision 2.0	A5503, A5507, A5510, A5513, A5520, A5521, A5524, A5526, A5530, A5533, A5536, A5661, A5664	Direction - Decrypt, Encrypt Key Length - 128, 256	SP 800-38E
Counter DRBG	A5503, A5505, A5506, A5507, A5508, A5509, A5510, A5511, A5512, A5513, A5514, A5515, A5521, A5522, A5523, A5526, A5528, A5529, A5530, A5531, A5532, A5533, A5534, A5535, A5536, A5537, A5538, A5661, A5662, A5663, A5664, A5665, A5666	Prediction Resistance - No, Yes Mode - AES-128, AES-192, AES-256 Derivation Function Enabled - Yes	SP 800-90A Rev. 1

Algorithm	CAVP Cert	Properties	Reference
ECDSA KeyGen (FIPS186-5)	A5503, A5526	Curve - P-256, P-384 Secret Generation Mode - testing candidates	FIPS 186-5
ECDSA SigVer (FIPS186-4)	A5504, A5527	Component - No Curve - P-256, P-384 Hash Algorithm - SHA-1	FIPS 186-4
ECDSA SigVer (FIPS186-5)	A5504, A5527	Curve - P-256, P-384 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512	FIPS 186-5
Hash DRBG	A5503, A5516, A5517, A5518, A5526, A5539, A5540, A5541, A5664	Prediction Resistance - No, Yes Mode - SHA-1, SHA2-256, SHA2-512	SP 800-90A Rev. 1
HMAC DRBG	A5503, A5516, A5517, A5518, A5526, A5539, A5540, A5541, A5664	Prediction Resistance - No, Yes Mode - SHA-1, SHA2-256, SHA2-512	SP 800-90A Rev. 1
HMAC-SHA-1	A5503, A5516, A5517, A5518, A5519, A5520, A5526, A5539, A5540, A5541, A5542, A5664	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-224	A5503, A5516, A5517, A5518, A5519, A5520, A5524, A5525, A5526, A5539, A5540, A5541, A5542, A5664	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-256	A5503, A5516, A5517, A5518, A5519, A5520, A5524, A5525, A5526, A5539, A5540, A5541, A5542, A5664	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-384	A5503, A5516, A5517, A5518, A5525, A5526, A5539, A5540, A5541, A5664	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-512	A5503, A5516, A5517, A5518, A5525, A5526, A5539, A5540, A5541, A5664	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA3-224	A5503, A5526, A5664	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1

Algorithm	CAVP Cert	Properties	Reference
HMAC-SHA3-256	A5503, A5526, A5664	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA3-384	A5503, A5526, A5664	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA3-512	A5503, A5526, A5664	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
KAS-ECC-SSC Sp800-56Ar3	A5503, A5526	Domain Parameter Generation Methods - P-256, P-384 Scheme - ephemeralUnified - KAS Role - initiator, responder	SP 800-56A Rev. 3
KAS-FFC-SSC Sp800-56Ar3	A5503, A5526	Domain Parameter Generation Methods - ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192 Scheme - dhEphem - KAS Role - initiator, responder	SP 800-56A Rev. 3
KDF SP800-108	A5503, A5526	KDF Mode - Counter Supported Lengths - Supported Lengths: 112-4096 Increment 8	SP 800-108 Rev. 1
RSA SigVer (FIPS186-4)	A5503, A5526, A5664	Signature Type - PKCS 1.5 Modulo - 2048, 3072, 4096	FIPS 186-4
RSA SigVer (FIPS186-5)	A5503, A5526, A5664	Modulo - 2048, 3072, 4096 Signature Type - pkcs1v1.5	FIPS 186-5
Safe Primes Key Generation	A5503, A5526	Safe Prime Groups - ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192	SP 800-56A Rev. 3

Algorithm	CAVP Cert	Properties	Reference
SHA-1	A5503, A5516, A5517, A5518, A5519, A5520, A5526, A5539, A5540, A5541, A5542, A5664	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2	FIPS 180-4
SHA2-224	A5503, A5516, A5517, A5518, A5519, A5520, A5524, A5525, A5526, A5539, A5540, A5541, A5542, A5664	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2	FIPS 180-4
SHA2-256	A5503, A5516, A5517, A5518, A5519, A5520, A5524, A5525, A5526, A5539, A5540, A5541, A5542, A5664	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2	FIPS 180-4
SHA2-384	A5503, A5516, A5517, A5518, A5525, A5526, A5539, A5540, A5541, A5664	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2	FIPS 180-4
SHA2-512	A5503, A5516, A5517, A5518, A5525, A5526, A5539, A5540, A5541, A5664	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2	FIPS 180-4
SHA3-224	A5503, A5526, A5664	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2	FIPS 202
SHA3-256	A5503, A5526, A5664	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2	FIPS 202
SHA3-384	A5503, A5526, A5664	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2	FIPS 202
SHA3-512	A5503, A5526, A5664	Message Length - Message Length: 0-	FIPS 202

Algorithm	CAVP Cert	Properties	Reference
		65536 Increment 8 Large Message Sizes - 1, 2	

Table 6: Approved Algorithms

Vendor-Affirmed Algorithms:

Name	Properties	Implementation	Reference
Asymmetric Cryptographic Key Generation (CKG)	Key Type:Asymmetric	N/A	SP 800-133 Rev. 2, section 4, example 1

Table 7: 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 with external IV (not compliant to FIPS 140-3 IG C.H)
KBKDF (by using the libkcapi)	Key derivation with implementation not tested by CAVP
HKDF (by using the libkcapi)	Key derivation with implementation not tested by CAVP
PBKDF2 (by using the libkcapi)	Password-based key derivation with implementation not tested by CAVP
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)
ECDSA	Signature generation (pre-hashed message); Signature verification (pre-hashed message)

Table 8: Non-Approved, Not Allowed Algorithms

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
Encryption with AES	BC-UnAuth	Encrypt a plaintext with AES	Key size (XTS):128, 256 bits Security strength (XTS):128, 256 bits Key size (Others):128, 192, 256 bits Security strength (Others):128, 192, 256 bits	AES-CBC: (A5503, A5507, A5510, A5513, A5520, A5521, A5524, A5526, A5530, A5533, A5536, A5661, A5664) AES-CBC-CS3: (A5503, A5507, A5510, A5513, A5520, A5521, A5526, A5530, A5533, A5536, A5664) AES-CFB128: (A5503, A5507, A5513, A5521, A5526, A5530, A5536, A5664) AES-CTR: (A5503, A5507, A5510, A5513, A5520, A5521, A5524, A5526, A5530,

Name	Type	Description	Properties	Algorithms
				A5533, A5536, A5661, A5664) AES-ECB: (A5503, A5505, A5506, A5507, A5508, A5509, A5510, A5511, A5512, A5513, A5514, A5515, A5520, A5521, A5522, A5523, A5524, A5526, A5528, A5529, A5530, A5531, A5532, A5533, A5534, A5535, A5536, A5537, A5538, A5661, A5662, A5663, A5664, A5665, A5666) AES-OFB: (A5503, A5507, A5513, A5521, A5526, A5530, A5536, A5664) AES-XTS Testing

Name	Type	Description	Properties	Algorithms
				Revision 2.0: (A5503, A5507, A5510, A5513, A5520, A5521, A5524, A5526, A5530, A5533, A5536, A5661, A5664)
Decryption with AES	BC-UnAuth	Decrypt a ciphertext with AES	Key size (XTS):128, 256 bits Security strength (XTS):128, 256 bits Key size (Others):128, 192, 256 bits Security strength (Others):128, 192, 256 bits	AES-CBC: (A5503, A5507, A5510, A5513, A5520, A5521, A5524, A5526, A5530, A5533, A5536, A5661, A5664) AES-CBC-CS3: (A5503, A5507, A5510, A5513, A5520, A5521, A5526, A5530, A5533, A5536, A5664) AES-CFB128: (A5503, A5507, A5513, A5521, A5526, A5530, A5536, A5664) AES-CTR:

Name	Type	Description	Properties	Algorithms
				(A5503, A5507, A5510, A5513, A5520, A5521, A5524, A5526, A5530, A5533, A5536, A5661, A5664) AES-ECB: (A5503, A5505, A5506, A5507, A5508, A5509, A5510, A5511, A5512, A5513, A5514, A5515, A5520, A5521, A5522, A5523, A5524, A5526, A5528, A5529, A5530, A5531, A5532, A5533, A5534, A5535, A5536, A5537, A5538, A5661, A5662, A5663, A5664, A5665, A5666) AES-OFB: (A5503,

Name	Type	Description	Properties	Algorithms
				A5507, A5513, A5521, A5526, A5530, A5536, A5664) AES-XTS Testing Revision 2.0: (A5503, A5507, A5510, A5513, A5520, A5521, A5524, A5526, A5530, A5533, A5536, A5661, A5664)
Message digest	SHA	Compute a message digest		SHA-1: (A5503, A5516, A5517, A5518, A5519, A5520, A5526, A5539, A5540, A5541, A5542, A5664) SHA2-224: (A5503, A5516, A5517, A5518, A5519, A5520, A5524, A5525, A5526, A5539, A5540, A5541, A5542,

Name	Type	Description	Properties	Algorithms
				A5664) SHA2-256: (A5503, A5516, A5517, A5518, A5519, A5520, A5524, A5525, A5526, A5539, A5540, A5541, A5542, A5664) SHA2-384: (A5503, A5516, A5517, A5518, A5525, A5526, A5539, A5540, A5541, A5664) SHA2-512: (A5503, A5516, A5517, A5518, A5525, A5526, A5539, A5540, A5541, A5664) SHA3-224: (A5503, A5526, A5664) SHA3-256: (A5503, A5526, A5664) SHA3-384: (A5503, A5526, A5664) SHA3-512:

Name	Type	Description	Properties	Algorithms
				(A5503, A5526, A5664)
Message authentication	MAC	Compute a MAC tag for authentication	Key size (HMAC):112-524288 bits Security strength (HMAC):112-256 bits Key size (AES):128, 192, 256 bits Security strength (AES):128, 192, 256 bits	AES-CMAC: (A5503, A5507, A5513, A5520, A5521, A5526, A5530, A5536, A5661, A5664) AES-GMAC: (A5503, A5507, A5513, A5521, A5526, A5530, A5536, A5661, A5664) HMAC-SHA-1: (A5503, A5516, A5517, A5518, A5519, A5520, A5526, A5539, A5540, A5541, A5542, A5664) HMAC-SHA2-224: (A5503, A5516, A5517, A5518, A5519, A5520, A5524, A5525, A5526, A5539, A5540, A5541,

Name	Type	Description	Properties	Algorithms
				A5542, A5664) HMAC-SHA2-256: (A5503, A5516, A5517, A5518, A5519, A5520, A5524, A5525, A5526, A5539, A5540, A5541, A5542, A5664) HMAC-SHA2-384: (A5503, A5516, A5517, A5518, A5525, A5526, A5539, A5540, A5541, A5664) HMAC-SHA2-512: (A5503, A5516, A5517, A5518, A5525, A5526, A5539, A5540, A5541, A5664) HMAC-SHA3-224: (A5503, A5526, A5664) HMAC-SHA3-256: (A5503, A5526, A5664) HMAC-SHA3-384: (A5503, A5526, A5664)

Name	Type	Description	Properties	Algorithms
				HMAC-SHA3-512: (A5503, A5526, A5664)
Random number generation with DRBGs	DRBG	Generate random numbers from DRBGs	CTR-DRBG:Modes: AES-128, AES-192, AES-256, with derivation function, with/without prediction resistance; Internal state length: 256, 320, 384 bits; Security strength: 128, 192, 256 bits HMAC-DRBG:Modes: SHA-1, SHA-256, SHA-512 with/without prediction resistance; Internal state length: 320, 512, 1024 bits; Security strength: 128, 256 bits Hash-DRBG:Modes: SHA-1, SHA-256, SHA-512 with/without prediction resistance; Internal state length: 880, 1776 bits; Security strength: 128, 256 bits	Counter DRBG: (A5503, A5505, A5506, A5507, A5508, A5509, A5510, A5511, A5512, A5513, A5514, A5515, A5521, A5522, A5523, A5526, A5528, A5529, A5530, A5531, A5532, A5533, A5534, A5535, A5536, A5537, A5538, A5661, A5662, A5663, A5664, A5665, A5666) Hash DRBG: (A5503, A5516, A5517, A5518, A5526, A5539, A5540, A5541, A5664) HMAC DRBG:

Name	Type	Description	Properties	Algorithms
				(A5503, A5516, A5517, A5518, A5526, A5539, A5540, A5541, A5664)
Authenticated encryption	BC-Auth	Encrypt and authenticate a plaintext	Key size (AES):128, 192, 256 bits Security strength (AES):128, 192, 256 bits	AES-CCM: (A5503, A5507, A5513, A5520, A5521, A5526, A5530, A5536, A5661, A5664) AES-GCM: (A5503, A5505, A5506, A5507, A5508, A5509, A5510, A5511, A5512, A5513, A5514, A5515, A5521, A5522, A5523, A5526, A5528, A5529, A5530, A5531, A5532, A5533, A5534, A5535, A5536, A5537, A5538, A5661, A5662,

Name	Type	Description	Properties	Algorithms
				A5663, A5664, A5665, A5666) AES-KW: (A5503, A5507, A5513, A5521, A5526, A5530, A5536, A5664) AES-CBC: (A5503, A5507, A5510, A5513, A5520, A5521, A5524, A5526, A5530, A5533, A5536, A5661, A5664) HMAC-SHA-1: (A5503, A5516, A5517, A5518, A5519, A5520, A5526, A5539, A5540, A5541, A5542, A5664) HMAC-SHA2-224: (A5503, A5516, A5517, A5518, A5519, A5520, A5526, A5539, A5540, A5541,

Name	Type	Description	Properties	Algorithms
				A5542, A5664) HMAC-SHA2-256: (A5503, A5516, A5517, A5518, A5519, A5520, A5526, A5539, A5540, A5541, A5542, A5664) HMAC-SHA2-384: (A5503, A5516, A5517, A5518, A5519, A5520, A5526, A5539, A5540, A5541, A5542, A5664) HMAC-SHA2-512: (A5503, A5516, A5517, A5518, A5519, A5520, A5526, A5539, A5540, A5541, A5542, A5664)
Authenticated decryption	BC-Auth	Decrypt and authenticate a ciphertext	Key size:128, 192, 256 bits Security strength:128, 192, 256 bits	AES-CCM: (A5503, A5507, A5513, A5520, A5521, A5526, A5530, A5536,

Name	Type	Description	Properties	Algorithms
				A5661, A5664) AES-GCM: (A5503, A5505, A5506, A5507, A5508, A5509, A5510, A5511, A5512, A5513, A5514, A5515, A5521, A5522, A5523, A5526, A5528, A5529, A5530, A5531, A5532, A5533, A5534, A5535, A5536, A5537, A5538, A5661, A5662, A5663, A5664, A5665, A5666) AES-KW: (A5503, A5507, A5513, A5521, A5526, A5530, A5536, A5664) AES-CBC: (A5503, A5507, A5510, A5513, A5520,

Name	Type	Description	Properties	Algorithms
				A5521, A5524, A5526, A5530, A5533, A5536, A5661, A5664) HMAC-SHA-1: (A5503, A5516, A5517, A5518, A5519, A5520, A5526, A5539, A5540, A5541, A5542, A5664) HMAC-SHA2-224: (A5503, A5516, A5517, A5518, A5519, A5520, A5526, A5539, A5540, A5541, A5542, A5664) HMAC-SHA2-256: (A5503, A5516, A5517, A5518, A5519, A5520, A5526, A5539, A5540, A5541, A5542, A5664) HMAC-SHA2-384: (A5503, A5516, A5517,

Name	Type	Description	Properties	Algorithms
				A5518, A5519, A5520, A5526, A5539, A5540, A5541, A5542, A5664) HMAC-SHA2-512: (A5503, A5516, A5517, A5518, A5519, A5520, A5526, A5539, A5540, A5541, A5542, A5664)
Key pair generation with ECDSA	AsymKeyPair-KeyGen CKG	Generate an asymmetric EC key pair	Curves:P-256, P-384 Security strength:128, 192 bits Mode:FIPS 186-5, Section A.2.2 - Rejection Sampling	ECDSA KeyGen (FIPS186-5): (A5503, A5526) Asymmetric Cryptographic Key Generation (CKG): ()
Key pair generation with Safe Primes	AsymKeyPair-KeyGen CKG	Generate an asymmetric DH key pair using Diffie-Hellman	Groups:ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192 Security strength:112-200 bits Mode:NIST SP 800-56A Rev. 3, Section 5.6.1.1.3 - Extra Random Bits	Safe Primes Key Generation: (A5503, A5526) Asymmetric Cryptographic Key Generation (CKG): ()
Digital signature verification with ECDSA	DigSig-SigVer	Verify a digital signature using ECDSA	Curves:P-256, P-384 Hashes:SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512 Security strength:80	ECDSA SigVer (FIPS186-4): (A5504, A5527) ECDSA SigVer

Name	Type	Description	Properties	Algorithms
			(SHA-1); 112, 128, 192, 256 bits (other hashes)	(FIPS186-5): (A5504, A5527)
Digital signature verification with RSA	DigSig-SigVer	Verify a signature with RSA	Padding:PKCS#1 v1.5 Hashes:SHA-256 Key size(s):4096 bits (149 bits)	RSA SigVer (FIPS186-4): (A5503, A5526, A5664) RSA SigVer (FIPS186-5): (A5503, A5526, A5664)
Shared secret computation with DH	KAS-SSC	Compute a shared secret using Diffie-Hellman	Groups:ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192 Security strength:112-200 bits KAS role:initiator, responder KAS Scheme:dhEphem	KAS-FFC-SSC Sp800-56Ar3: (A5503, A5526)
Shared secret computation with ECDH	KAS-SSC	Compute a shared secret using Elliptic Curve Diffie-Hellman	Curves:P-256, P-384 Security strength:128, 192 bits KAS role:initiator, responder KAS scheme:ephemeralUnified	KAS-ECC-SSC Sp800-56Ar3: (A5503, A5526)
Key derivation with KBKDF	KBKDF	Derive a symmetric key from a key-derivation key	KDF mode:Counter MAC mode:AES-CMAC with 128-, 192-, 256-bit keys; HMAC with SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA3-224, SHA3-256, SHA3-384, SHA3-512 Derived key length:112-4096 bits Security strength:112-256 bits	KDF SP800-108: (A5503, A5526)

Table 9: Security Function Implementations

2.7 Algorithm Specific Information

2.7.1 AES GCM IV

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

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

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

The design of the IPsec protocol implicitly ensures that the counter (the nonce_explicit part of the IV) does not exhaust the maximum number of possible values for a given session key.

In the event the module's power is lost and restored, the consuming application must ensure that a new key for use with the AES GCM key encryption or decryption under this scenario shall be established.

The module also provides a non-approved AES GCM encryption service which accepts arbitrary external IVs from the operator. This service can be requested by invoking the crypto_aead_encrypt API function with an AES GCM handle.

Any approved use of the AES GCM service is indicated by the crypto_aead_get_flags(tfm) API returning the CRYPTO_TFM_FIPS_COMPLIANCE flag, as described in section 4.3.

2.7.2 AES XTS

The length of a single data unit encrypted or decrypted with AES XTS shall not exceed 2^{20} AES blocks, that is 16MB, of data per XTS instance. An XTS instance is defined in Section 4 of SP 800-38E. To meet the requirement stated in IG C.I, the module implements a check to ensure that the two AES keys used in AES XTS mode are not identical. As the module does not implement symmetric key generation, this check is performed when the keys are input by the operator. Key_1 and Key_2 shall be generated and/or established independently according to the rules for component symmetric keys from NIST SP 800-133r2, Section 6.3.

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

2.7.3 RSA

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

2.7.4 SP 800-56A Rev. 3 Assurances

To comply with the assurances found in Section 5.6.2 of SP 800-56A Rev. 3, the operator must use the Diffie-Hellman and EC Diffie-Hellman shared secret computation algorithms in the context of IETF protocols. Additionally, the module's approved key pair generation service (see Approved Services table in Section 4.3 Approved Services) must be used to generate ephemeral Diffie-Hellman or EC Diffie-Hellman key pairs, or the key pairs must be obtained from another FIPS-validated module. As part of this service, the module will internally perform the full public key validation of the generated public key.

The module's shared secret computation service will internally perform the full public key validation of the peer public key, complying with Sections 5.6.2.2.1 and 5.6.2.2.2 of SP 800-56A Rev. 3.

2.7.5 Key Agreement

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.

2.7.6 Key Transport

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

2.7.7 SHA-1

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

2.8 RBG and Entropy[1]

Cert Number	Vendor Name
E206	SUSE LLC
E211	SUSE LLC

Table 10: Entropy Certificates

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
SUSE Kernel CPU Time Jitter RNG	Non-Physical	SUSE Linux Enterprise Server 15 SP6 on AMD EPYC(TM) 7343; SUSE Linux Enterprise Server 15 SP6 on Ampere® Altra® Q80-30; SUSE Linux Enterprise Server 15 SP6 on IBM® Telum(TM); SUSE Linux Enterprise Server 15 SP6 on Intel® Xeon® Gold 5416S	256 bits	Full entropy	SHA3-256 (A5503)
SUSE Kernel-RT CPU Time	Non-Physical	SUSE Linux Enterprise Server 15 SP6 on AMD EPYC(TM) 7343; SUSE Linux Enterprise	256 bits	Full entropy	SHA3-256 (A5526)

[1] The kernel RT and kernel-default modules are compiled within different binaries. For this reason, two separate ESV validations were performed. Entropy-related source code between the two versions the kernel is the same.

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
Jitter RNG		Server 15 SP6 on Intel® Xeon® Gold 5416S			

Table 11: Entropy Sources

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

Additionally, the module employs a specific HMAC-SHA2-512 DRBG implementation for internal purposes (e.g. to generate initialization vectors). This DRBG is initially seeded with 384 output bits from the entropy source (384 bits of entropy) and reseeded with 256 output bits from the entropy source (256 bits of entropy). Outputs of multiple GetEntropy() calls are concatenated to receive the entropy input length greater than 256 bits. The output is truncated to get the entropy input string which is not a multiple of 256.

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

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

2.9 Key Generation

The module implements asymmetric key pair generation compliant with SP 800-133 Rev. 2. When random values are required, they are obtained from the SP 800-90A Rev. 1 approved DRBG, compliant with Section 4 of SP 800-133 Rev. 2 (without XOR):

- Safe primes key pair generation: compliant with SP 800-133 Rev. 2, Section 5.2, which maps to SP 800-56A Rev. 3. The method described in Section 5.6.1.1.4 of SP 800-56A Rev. 3 (“Testing Candidates”) is used.
- ECC (ECDH and ECDSA) key pair generation: compliant with SP 800-133 Rev. 2, Section 5.1, which maps to FIPS 186-5. The method described in Appendix A.2.2 of FIPS 186-5 (“Rejection Sampling”) is used.

Additionally, the module implements the following key derivation methods:

- KBKDF: compliant with SP 800-108 Rev. 1. This implementation can be used to generate secret keys from a pre-existing key-derivation-key.

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 shared secret computation as listed in the Security Function Implementations table in 2.6 Security Function Implementations.

2.11 Industry Protocols

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

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

Physical Port	Logical Interface(s)	Data That Passes
N/A	Data Input	API data input parameters, AF_ALG type sockets
N/A	Data Output	API data output parameters, AF_ALG type sockets
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 12: Ports and Interfaces

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

4 Roles, Services, and Authentication

4.1 Authentication Methods

The module does not implement authentication.

4.2 Roles

Name	Type	Operator Type	Authentication Methods
Crypto Officer	Role	CO	None

Table 13: Roles

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	Crypto Officer
Encryption	Encrypt a plaintext	crypto_skcipher_setkey returns 0	AES key, plaintext	Ciphertext	Encryption with AES	Crypto Officer - AES key: W,E
Decryption	Decrypt a ciphertext	crypto_skcipher_setkey returns 0	AES key, ciphertext	Plaintext	Decryption with AES	Crypto Officer - AES key: W,E
Authenticated encryption	Encrypt and authenticate a plaintext	For all except AES GCM: crypto_aead_setkey returns 0; For AES GCM: crypto_aead_get_flags(tfm) has the CRYPTO_TFM_FIPS_COMPLIANCE flag set	AES key, plaintext, IV	Ciphertext, MAC tag	Authenticated encryption	Crypto Officer - AES key: W,E
Authenticated	Decrypt an authenti	For all except AES GCM: crypto_aead_setkey returns 0; For AES GCM:	AES key, ciphert	Plaintext or failure	Authenticated	Crypto Officer - AES

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
decryption	cated ciphertext	crypto_aead_get_flags(tfm) has the CRYPTO_TFM_FIPS_COMPLIANCE flag set	ext, MAC tag, IV		decryption	key: W,E
Encrypt then MAC	Encrypt plaintext with AES and use HMAC authenticate it	crypto_shash_init returns 0	AES key, HMAC key, plaintext	Ciphertext, MAC tag	Authenticated encryption	Crypto Officer - AES key: W,E - HMAC key: W,E
Decrypt then verify	Decrypt an authenticated a ciphertext using AES and HMAC	crypto_shash_init returns 0	AES key, HMAC key, ciphertext, MAC tag	Plaintext or failure	Authenticated decryption	Crypto Officer - AES key: W,E - HMAC key: W,E
Message authentication generation	Compute a MAC tag	crypto_shash_init returns 0	AES: AES key, message; HMAC: HMAC key, message	MAC tag	Message authentication	Crypto Officer - AES key: W,E - HMAC key: W,E
Message authentication verification	Compute a MAC tag	crypto_shash_init returns 0	AES: AES key, message, MAC tag; HMAC: HMAC key, message,	Success/Failure	Message authentication	Crypto Officer - AES key: W,E - HMAC key: W,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
			MAC tag			
Random number generation	Generate random bytes	crypto_rng_get_bytes returns 0	Output length	Random bytes	Random number generation with DRBGs	Crypto Officer - Entropy input: W,E,Z - CTR_DRBG seed: G,E,Z - Hash_DRBG seed: G,E,Z - HMAC_DRBG seed: G,E,Z - CTR_DRBG Internal state (V, Key): G,W,E - Hash_DRBG Internal state (V, C): G,W,E - HMAC_DRBG Internal state (V, Key): G,W,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Key derivation	Derive a symmetric key from a key-derivation key	crypto_kdf108_ctr_generate returns 0	Output length	Derived key	Key derivation with KBKDF	Crypto Officer - Key-derivation key: W,E - Derived key: G,R
DH Key pair generation	Generate an asymmetric DH key pair using Diffie-Hellman	crypto_kpp_set_secret() and crypto_kpp_generate_public_key() return 0	Group	DH key pair	Key pair generation with Safe Primes	Crypto Officer - Module-generated DH private key: G,R - Module-generated DH public key: G,R - Intermediate key generation value: G,E,Z
EC Key pair generation	Generate an asymmetric EC key pair	crypto_kpp_set_secret() and crypto_kpp_generate_public_key() return 0	Curve	EC key pair	Key pair generation with ECDSA	Crypto Officer - Module-generated EC private key: G,R - Module-generat

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						ed EC public key: G,R - Intermediate key generation value: G,E,Z
Shared secret computation	Compute a shared secret using (EC) Diffie-Hellman	crypto_kpp_compute_shared_secret() returns 0	Public key (peer), Private key	Shared secret	Shared secret computation with DH Shared secret computation with ECDH	Crypto Officer - DH private key: W,E - DH public key: W,E - EC private key: W,E - EC public key: W,E - Shared secret: G,R
Error detection code	Compute an EDC (crc32, crct10dif)	None	Message	EDC	None	Crypto Officer
Compression	Compress data (deflate, lz4, lz4hc, lzo,	None	Data	Compressed data	None	Crypto Officer

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	zlibdeflate, 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 with AES Decryption with AES Message digest Message authentication Random number generation with DRBGs Authenticated encryption Authenti	Crypto Officer

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					cated decryption Digital signature verification with ECDSA Digital signature verification with RSA Shared secret computation with DH Shared secret computation with ECDH Key derivation with KBKDF	
Zeroization	Zeroize all SSPs	None	Any SSP	N/A	None	Crypto Officer - AES key: Z - HMAC key: Z - Entropy input: Z - CTR_DRBG Internal state (V, Key): Z - Hash_DRBG Internal state

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						(V, C): Z - HMAC_DRBG Internal state (V, Key): Z - CTR_DRBG seed: Z - Hash_DRBG seed: Z - HMAC_DRBG seed: Z - Key-derivation key: Z - Derived key: Z - Intermediate key generation value: Z - Module-generated DH private key: Z - Module-generated DH public key: Z - Module-generat

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						ed EC private key: Z - Module-generated EC public key: Z - DH private key: Z - DH public key: Z - EC private key: Z - EC public key: Z - Shared secret: Z

Table 14: Approved Services

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

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

4.4 Non-Approved Services

Name	Description	Algorithms	Role
AES GCM external IV encryption	Encrypt a plaintext using AES GCM with an external IV	AES-GCM with external IV	CO
Key derivation	Derive a key from a key-derivation key or a shared secret	KBKDF (by using the libkcapi) HKDF (by using the libkcapi)	CO

Name	Description	Algorithms	Role
Password-based key derivation	Derive a key from a password	PBKDF2 (by using the libkcapi)	CO
RSA encryption primitive	Compute the raw RSA encryption of a plaintext	RSA	CO
RSA decryption primitive	Compute the raw RSA decryption of a ciphertext	RSA	CO
RSA signature generation (pre-hashed message)	Generate a digital signature for a pre-hashed message	RSA with PKCS#1 v1.5 padding ECDSA	CO
RSA signature verification (pre-hashed message)	Verify a digital signature for a pre-hashed message	RSA with PKCS#1 v1.5 padding ECDSA	CO

Table 15: Non-Approved Services

4.5 External Software/Firmware Loaded

The module does not load external software or firmware.

5 Software/Firmware Security

5.1 Integrity Techniques

The Linux kernel binary is integrity tested using an HMAC-SHA2-256 calculation performed by the fipscheck application (which utilizes the module's HMAC and SHA-256 implementations). An HMAC-SHA2-256 calculation is also performed on the fipscheck application and the libkcapi library to verify their integrity. The kernel crypto object files listed in section 2.2 are loaded on start-up by the module and verified using RSA signature verification with PKCS#1 v1.5 padding, SHA-256, and a 4096-bit key.

The fipscheck application first executes the HMAC-SHA2-256 self-test. After this self-test is successful, the fipscheck application is used to perform an HMAC calculation of the libkcapi library, the kernel binary, and of its own binary to verify their integrity.

After the integrity of these components has been verified, the self-test for the RSA signature verification implementation is run. Upon successful run of this self-test, the RSA signature verification implementation of the kernel is used to verify the integrity of the crypto object files listed in section 2.2 and loaded at start-up.

5.2 Initiate on Demand

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

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Modifiable

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

6.2 Configuration Settings and Restrictions

The module shall be installed as stated in Section 11.1.

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

7 Physical Security

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

8 Non-Invasive Security

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

9 Sensitive Security Parameters Management

9.1 Storage Areas

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

Table 16: 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
AF_ALG_type sockets (input)	Operator calling application (TOEPP), userspace	Cryptographic module	Plaintext	Manual	Electronic	
AF_ALG_type sockets (output)	Cryptographic module	Operator calling application (TOEPP), userspace	Plaintext	Manual	Electronic	
API input parameters (input)	Operator calling application (TOEPP), kernel space	Cryptographic module	Plaintext	Manual	Electronic	
API output parameters (output)	Cryptographic module	Operator calling application (TOEPP), kernel space	Plaintext	Manual	Electronic	

Table 17: SSP Input-Output Methods

9.3 SSP Zeroization Methods

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

Table 18: 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	128, 192, 256	Symmetric Key - CSP			Encryption with AES

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	encryption, decryption, and computing MAC tags.	bits - 128, 192, 256 bits				Decryption with AES Message authentication Authenticated encryption Authenticated decryption
HMAC key	HMAC key.	112-524288 bits - 112-256 bits	Authentication key - CSP			Message authentication
Entropy input	Entropy input used to seed the DRBGs. Compliant with IG D.L.	128-384 bits - 128-384 bits	Entropy input - CSP			Random number generation with DRBGs
CTR_DRBG seed	DRBG seed derived from entropy input. Compliant with IG D.L.	256, 320, 384 bits - 128, 192, 256 bits	Seed - CSP	Random number generation with DRBGs		Random number generation with DRBGs
Hash_DRBG seed	DRBG seed derived from entropy input. Compliant with IG D.L.	440, 888 bits - 128, 256 bits	Seed - CSP	Random number generation with DRBGs		Random number generation with DRBGs

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
HMAC_DRBG seed	DRBG seed derived from entropy input. Compliant with IG D.L.	440, 888 bits - 128, 256 bits	Seed - CSP	Random number generation with DRBGs		Random number generation with DRBGs
CTR_DRBG Internal state (V, Key)	Internal state of CTR_DRBG instances. Compliant with IG D.L.	256, 320, 384 bits - 128, 192, 256 bits	Internal state - CSP	Random number generation with DRBGs		Random number generation with DRBGs
Hash_DRBG Internal state (V, C)	Internal state of Hash_DRBG instances. Compliant with IG D.L.	880, 1776 bits - 128, 256 bits	Internal state - CSP	Random number generation with DRBGs		Random number generation with DRBGs
HMAC_DRBG Internal state (V, Key)	Internal state of HMAC_DRBG instances. Compliant with IG D.L.	320, 512, 1024 bits - 128, 256 bits	Internal state - CSP	Random number generation with DRBGs		Random number generation with DRBGs
Key-derivation key	Symmetric key used to derive symmetric keys	112-4096 bits - 112-256 bits	Symmetric key - CSP			Key derivation with KBKDF
Derived key	Symmetric key derived from a key-	112-4096 bits - 112-256 bits	Symmetric key - CSP	Key derivation with KBKDF		Key derivation with KBKDF

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	derivation key					
Intermediate key generation value	Intermediate key pair generation value generated during key generation services (SP 800-133 Rev. 2 Section 4, 5.1, and 5.2)	112-8912 bits - 112-256 bits	Intermediate value - CSP	Key pair generation with ECDSA Key pair generation with Safe Primes		Key pair generation with ECDSA Key pair generation with Safe Primes
Module-generated DH private key	DH private key generated by the module	ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192 - 112-200 bits	Private key - CSP	Key pair generation with Safe Primes		Key pair generation with Safe Primes
Module-generated DH public key	DH public key generated by the module	ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192 - 112-200 bits	Public key - PSP	Key pair generation with Safe Primes		Key pair generation with Safe Primes
Module-generated EC private key	EC private key generated by the module	P-256, P-384 - 128, 192 bits	Private key - CSP	Key pair generation with ECDSA		Key pair generation with ECDSA

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
Module-generated EC public key	EC public key generated by the module	P-256, P-384 - 128, 192 bits	Public key - PSP	Key pair generation with ECDSA		Key pair generation with ECDSA
DH private key	DH private key input to the module and used for shared secret computation	ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192 - 112-200 bits	Private key - CSP			Shared secret computation with DH
DH public key	DH public key input to the module and used for shared secret computation	ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192 - 112-200 bits	Public key - PSP			Shared secret computation with DH
EC private key	ECDH private key input to the module and used for shared secret computation	P-256, P-384 - 128, 192 bits	Private key - CSP			Shared secret computation with ECDH
EC public key	ECDH public key input to the module and used for shared	P-256, P-384 - 128, 192 bits	Public key - PSP			Shared secret computation with ECDH

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	secret computation					
Shared secret	Shared secret generated by ECDH/DH shared secret computation	224-8912 bits - 112-256 bits	Shared Secret - CSP		Shared secret computation with DH Shared secret computation with ECDH	Shared secret computation with DH Shared secret computation with ECDH Key derivation with KBKDF

Table 19: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
AES key	AF_ALG_type sockets (input) API input parameters (input)	RAM:Plaintext	Until cipher handle is freed or module powered off	Free cipher handle Remove power from the module	
HMAC key	AF_ALG_type sockets (input) API input parameters (input)	RAM:Plaintext	Until cipher handle is freed or module powered off	Free cipher handle Remove power from the module	
Entropy input		RAM:Plaintext	From generation until DRBG seed/reseed	Automatic	CTR_DRBG Seed:Derives Hash_DRBG Seed:Derives HMAC_DRBG Seed:Derives
CTR_DRBG seed		RAM:Plaintext	While the DRBG is being instantiated	Automatic	Entropy input:Derived From CTR_DRBG

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
					Internal state (V, Key):Derives
Hash_DRBG seed		RAM:Plaintext	While the DRBG is being instantiated	Automatic	Entropy input:Derived From Hash_DRBG Internal state (V, C):Derives
HMAC_DRBG seed		RAM:Plaintext	While the DRBG is being instantiated	Automatic	Entropy input:Derived From HMAC_DRBG Internal state (V, Key):Derives
CTR_DRBG Internal state (V, Key)		RAM:Plaintext	From DRBG instantiation until DRBG is un-instantiated	Free cipher handle Remove power from the module	CTR_DRBG seed:Derived From
Hash_DRBG Internal state (V, C)		RAM:Plaintext	From DRBG instantiation until DRBG is un-instantiated	Free cipher handle Remove power from the module	Hash_DRBG seed:Derived From
HMAC_DRBG Internal state (V, Key)		RAM:Plaintext	From DRBG instantiation until DRBG is un-instantiated	Free cipher handle Remove power from the module	HMAC_DRBG seed:Derived From
Key-derivation key	API input parameters (input)	RAM:Plaintext	From service invocation until cipherhandle is freed	Free cipher handle Remove power from the module	Derived key:Derives
Derived key	API output parameters (output)	RAM:Plaintext	From service invocation until cipherhandle is freed	Free cipher handle Remove power from the module	Key-derivation key:Derived From

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
Intermediate key generation value		RAM:Plaintext	From service invocation until it is completed	Automatic Remove power from the module	Module-generated DH private key:Generates Module-generated DH public key:Generates Module-generated EC private key:Generates Module-generated EC public key:Generates
Module-generated DH private key	AF_ALG_type sockets (output) API output parameters (output)	RAM:Plaintext	Until cipher handle is freed or module powered off	Free cipher handle Remove power from the module	Intermediate key generation value:Generated from Module-generated DH public key:Paired With
Module-generated DH public key	AF_ALG_type sockets (output) API output parameters (output)	RAM:Plaintext	Until cipher handle is freed or module powered off	Free cipher handle Remove power from the module	Intermediate key generation value:Generated from Module-generated DH private key:Paired With
Module-generated EC private key	AF_ALG_type sockets (output) API output parameters (output)	RAM:Plaintext	Until cipher handle is freed or module powered off	Free cipher handle Remove power from the module	Intermediate key generation value:Generated From Module-generated EC public key:Paired With
Module-generated EC public key	AF_ALG_type sockets (output) API output	RAM:Plaintext	Until cipher handle is freed or	Free cipher handle Remove	Intermediate key generation value:Generated From Module-

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	parameters (output)		module powered off	power from the module	generated EC private key:Paired With
DH private key	AF_ALG_type sockets (input) API input parameters (input)	RAM:Plaintext		Free cipher handle Remove power from the module	DH public key:Paired With Shared secret:Establishes
DH public key	AF_ALG_type sockets (input) API input parameters (input)	RAM:Plaintext		Free cipher handle Remove power from the module	DH private key:Paired With Shared secret:Establishes
EC private key	AF_ALG_type sockets (input) API input parameters (input)	RAM:Plaintext		Free cipher handle Remove power from the module	EC public key:Paired With Shared secret:Establishes
EC public key	AF_ALG_type sockets (input) API input parameters (input)	RAM:Plaintext		Free cipher handle Remove power from the module	EC private key:Paired With Shared secret:Establishes
Shared secret	AF_ALG_type sockets (output) API output parameters (output)	RAM:Plaintext	From service invocation until cipherhandle is freed	Free cipher handle Remove power from the module	DH private key:Established By DH public key:Established By EC private key:Established By EC public key:Established By

Table 20: SSP Table 2

9.5 Transitions

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

10 Self-Tests

10.1 Pre-Operational Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
HMAC-SHA2-256 (A5503) - kernel version 3.5	256-bit key	Message Authentication	SW/FW Integrity	Module becomes operational and services are available for use.	Integrity test for kernel binary version 3.5
HMAC-SHA2-256 (A5503) - fipscheck version 3.5	256-bit key	Message Authentication	SW/FW Integrity	Module becomes operational and services are available for use.	Integrity test for fipscheck application version 3.5
RSA SigVer (FIPS186-5) (A5503) - object files version 3.5	4096-bit key with SHA2-256	Signature Verification	SW/FW Integrity	Module becomes operational and services are available for use.	Integrity test for kernel object files version 3.5
HMAC-SHA2-256 (A5526) - kernel version 3.6	256-bit key	Message Authentication	SW/FW Integrity	Module becomes operational and services are available for use.	Integrity test for kernel binary version 3.6
HMAC-SHA2-256 (A5526) - fipscheck version 3.6	256-bit key	Message Authentication	SW/FW Integrity	Module becomes operational and services are available for use.	Integrity test for fipscheck application version 3.6
RSA SigVer (FIPS186-5) (A5526) - object files version 3.6	4096-bit key with SHA2-256	Signature Verification	SW/FW Integrity	Module becomes operational and services are available for use.	Integrity test for kernel object files version 3.6

Table 21: Pre-Operational Self-Tests

The pre-operational software integrity tests are performed automatically when the module is powered on, before the module transitions into the operational state. The algorithms used for the integrity test (i.e., HMAC-SHA2-256 and RSA SigVer with 4096 bit key) run their CASTs before the integrity test is performed. While the module is executing the self-tests, services are not available, and data output (via the data output interface) is inhibited until the pre-operational software integrity self-tests are successfully completed. The module transitions to the operational state only after the pre-operational self-tests are passed successfully.

10.2 Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
SHA-1 (A5503)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are available for use.	Message Digest	Module initialization
SHA-1 (A5516)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are available for use.	Message Digest	Module initialization
SHA-1 (A5517)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are available for use.	Message Digest	Module initialization
SHA-1 (A5518)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are available for use.	Message Digest	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
SHA-1 (A5519)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are available for use.	Message Digest	Module initialization
SHA-1 (A5520)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are available for use.	Message Digest	Module initialization
SHA-1 (A5526)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are available for use.	Message Digest	Module initialization
SHA-1 (A5539)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are available for use.	Message Digest	Module initialization
SHA-1 (A5540)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are available for use.	Message Digest	Module initialization
SHA-1 (A5541)	0-8184 bit messages	KAT	CAST	Module becomes operationa	Message Digest	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				l and services are available for use.		
SHA-1 (A5542)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are available for use.	Message Digest	Module initialization
SHA-1 (A5664)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are available for use.	Message Digest	Module initialization
SHA2-256 (A5503)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are available for use.	Message Digest	Module initialization
SHA2-256 (A5516)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are available for use.	Message Digest	Module initialization
SHA2-256 (A5517)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are	Message Digest	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				available for use.		
SHA2-256 (A5518)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are available for use.	Message Digest	Module initialization
SHA2-256 (A5519)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are available for use.	Message Digest	Module initialization
SHA2-256 (A5520)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are available for use.	Message Digest	Module initialization
SHA2-256 (A5524)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are available for use.	Message Digest	Module initialization
SHA2-256 (A5525)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are available for use.	Message Digest	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
SHA2-256 (A5526)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are available for use.	Message Digest	Module initialization
SHA2-256 (A5539)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are available for use.	Message Digest	Module initialization
SHA2-256 (A5540)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are available for use.	Message Digest	Module initialization
SHA2-256 (A5541)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are available for use.	Message Digest	Module initialization
SHA2-256 (A5542)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are available for use.	Message Digest	Module initialization
SHA2-256 (A5664)	0-8184 bit messages	KAT	CAST	Module becomes operationa	Message Digest	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				l and services are available for use.		
SHA2-512 (A5503)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are available for use.	Message Digest	Module initialization
SHA2-512 (A5516)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are available for use.	Message Digest	Module initialization
SHA2-512 (A5517)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are available for use.	Message Digest	Module initialization
SHA2-512 (A5518)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are available for use.	Message Digest	Module initialization
SHA2-512 (A5525)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are	Message Digest	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				available for use.		
SHA2-512 (A5526)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are available for use.	Message Digest	Module initialization
SHA2-512 (A5539)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are available for use.	Message Digest	Module initialization
SHA2-512 (A5540)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are available for use.	Message Digest	Module initialization
SHA2-512 (A5541)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are available for use.	Message Digest	Module initialization
SHA2-512 (A5664)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are available for use.	Message Digest	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
SHA3-224 (A5503)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are available for use.	Message Digest	Module initialization
SHA3-224 (A5526)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are available for use.	Message Digest	Module initialization
SHA3-224 (A5664)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are available for use.	Message Digest	Module initialization
SHA3-256 (A5503)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are available for use.	Message Digest	Module initialization
SHA3-256 (A5526)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are available for use.	Message Digest	Module initialization
SHA3-256 (A5664)	0-8184 bit messages	KAT	CAST	Module becomes operationa	Message Digest	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				l and services are available for use.		
SHA3-384 (A5503)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are available for use.	Message Digest	Module initialization
SHA3-384 (A5526)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are available for use.	Message Digest	Module initialization
SHA3-384 (A5664)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are available for use.	Message Digest	Module initialization
SHA3-512 (A5503)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are available for use.	Message Digest	Module initialization
SHA3-512 (A5526)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are	Message Digest	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				available for use.		
SHA3-512 (A5664)	0-8184 bit messages	KAT	CAST	Module becomes operational and services are available for use.	Message Digest	Module initialization
AES-GCM - Encrypt (A5503)	128, 192, 256 bit keys and 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Encryption	Module initialization
AES-GCM - Encrypt (A5505)	128, 192, 256 bit keys and 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Encryption	Module initialization
AES-GCM - Encrypt (A5506)	128, 192, 256 bit keys and 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Encryption	Module initialization
AES-GCM - Encrypt (A5507)	128, 192, 256 bit keys and 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Encryption	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-GCM - Encrypt (A5508)	128, 192, 256 bit keys and 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Encryption	Module initialization
AES-GCM - Encrypt (A5509)	128, 192, 256 bit keys and 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Encryption	Module initialization
AES-GCM - Encrypt (A5510)	128, 192, 256 bit keys and 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Encryption	Module initialization
AES-GCM - Encrypt (A5511)	128, 192, 256 bit keys and 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Encryption	Module initialization
AES-GCM - Encrypt (A5512)	128, 192, 256 bit keys and 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Encryption	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-GCM - Encrypt (A5513)	128, 192, 256 bit keys and 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Encryption	Module initialization
AES-GCM - Encrypt (A5514)	128, 192, 256 bit keys and 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Encryption	Module initialization
AES-GCM - Encrypt (A5515)	128, 192, 256 bit keys and 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Encryption	Module initialization
AES-GCM - Encrypt (A5521)	128, 192, 256 bit keys and 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Encryption	Module initialization
AES-GCM - Encrypt (A5522)	128, 192, 256 bit keys and 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Encryption	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-GCM - Encrypt (A5523)	128, 192, 256 bit keys and 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Encryption	Module initialization
AES-GCM - Encrypt (A5526)	128, 192, 256 bit keys and 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Encryption	Module initialization
AES-GCM - Encrypt (A5528)	128, 192, 256 bit keys and 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Encryption	Module initialization
AES-GCM - Encrypt (A5529)	128, 192, 256 bit keys and 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Encryption	Module initialization
AES-GCM - Encrypt (A5530)	128, 192, 256 bit keys and 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Encryption	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-GCM - Encrypt (A5531)	128, 192, 256 bit keys and 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Encryption	Module initialization
AES-GCM - Encrypt (A5532)	128, 192, 256 bit keys and 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Encryption	Module initialization
AES-GCM - Encrypt (A5533)	128, 192, 256 bit keys and 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Encryption	Module initialization
AES-GCM - Encrypt (A5534)	128, 192, 256 bit keys and 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Encryption	Module initialization
AES-GCM - Encrypt (A5535)	128, 192, 256 bit keys and 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Encryption	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-GCM - Encrypt (A5536)	128, 192, 256 bit keys and 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Encryption	Module initialization
AES-GCM - Encrypt (A5537)	128, 192, 256 bit keys and 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Encryption	Module initialization
AES-GCM - Encrypt (A5538)	128, 192, 256 bit keys and 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Encryption	Module initialization
AES-GCM - Encrypt (A5661)	128, 192, 256 bit keys and 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Encryption	Module initialization
AES-GCM - Encrypt (A5662)	128, 192, 256 bit keys and 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Encryption	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-GCM - Encrypt (A5663)	128, 192, 256 bit keys and 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Encryption	Module initialization
AES-GCM - Encrypt (A5664)	128, 192, 256 bit keys and 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Encryption	Module initialization
AES-GCM - Encrypt (A5665)	128, 192, 256 bit keys and 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Encryption	Module initialization
AES-GCM - Encrypt (A5666)	128, 192, 256 bit keys and 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Encryption	Module initialization
AES-GCM - Decrypt (A5503)	128, 192, 256 bit keys and 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Decryption	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-GCM - Decrypt (A5505)	128, 192, 256 bit keys and 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Decryption	Module initialization
AES-GCM - Decrypt (A5506)	128, 192, 256 bit keys and 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Decryption	Module initialization
AES-GCM - Decrypt (A5507)	128, 192, 256 bit keys and 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Decryption	Module initialization
AES-GCM - Decrypt (A5508)	128, 192, 256 bit keys and 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Decryption	Module initialization
AES-GCM - Decrypt (A5509)	128, 192, 256 bit keys and 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Decryption	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-GCM - Decrypt (A5510)	128, 192, 256 bit keys and 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Decryption	Module initialization
AES-GCM - Decrypt (A5511)	128, 192, 256 bit keys and 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Decryption	Module initialization
AES-GCM - Decrypt (A5512)	128, 192, 256 bit keys and 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Decryption	Module initialization
AES-GCM - Decrypt (A5513)	128, 192, 256 bit keys and 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Decryption	Module initialization
AES-GCM - Decrypt (A5514)	128, 192, 256 bit keys and 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Decryption	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-GCM - Decrypt (A5515)	128, 192, 256 bit keys and 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Decryption	Module initialization
AES-GCM - Decrypt (A5521)	128, 192, 256 bit keys and 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Decryption	Module initialization
AES-GCM - Decrypt (A5522)	128, 192, 256 bit keys and 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Decryption	Module initialization
AES-GCM - Decrypt (A5523)	128, 192, 256 bit keys and 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Decryption	Module initialization
AES-GCM - Decrypt (A5526)	128, 192, 256 bit keys and 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Decryption	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-GCM - Decrypt (A5528)	128, 192, 256 bit keys and 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Decryption	Module initialization
AES-GCM - Decrypt (A5529)	128, 192, 256 bit keys and 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Decryption	Module initialization
AES-GCM - Decrypt (A5530)	128, 192, 256 bit keys and 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Decryption	Module initialization
AES-GCM - Decrypt (A5531)	128, 192, 256 bit keys and 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Decryption	Module initialization
AES-GCM - Decrypt (A5532)	128, 192, 256 bit keys and 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Decryption	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-GCM - Decrypt (A5533)	128, 192, 256 bit keys and 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Decryption	Module initialization
AES-GCM - Decrypt (A5534)	128, 192, 256 bit keys and 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Decryption	Module initialization
AES-GCM - Decrypt (A5535)	128, 192, 256 bit keys and 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Decryption	Module initialization
AES-GCM - Decrypt (A5536)	128, 192, 256 bit keys and 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Decryption	Module initialization
AES-GCM - Decrypt (A5537)	128, 192, 256 bit keys and 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Decryption	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-GCM - Decrypt (A5538)	128, 192, 256 bit keys and 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Decryption	Module initialization
AES-GCM - Decrypt (A5661)	128, 192, 256 bit keys and 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Decryption	Module initialization
AES-GCM - Decrypt (A5662)	128, 192, 256 bit keys and 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Decryption	Module initialization
AES-GCM - Decrypt (A5663)	128, 192, 256 bit keys and 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Decryption	Module initialization
AES-GCM - Decrypt (A5664)	128, 192, 256 bit keys and 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Decryption	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-GCM - Decrypt (A5665)	128, 192, 256 bit keys and 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Decryption	Module initialization
AES-GCM - Decrypt (A5666)	128, 192, 256 bit keys and 96-bit IVs	KAT	CAST	Module becomes operational and services are available for use.	Decryption	Module initialization
AES-ECB - Encrypt (A5503)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Encryption	Module initialization
AES-ECB - Encrypt (A5505)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Encryption	Module initialization
AES-ECB - Encrypt (A5506)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Encryption	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-ECB - Encrypt (A5507)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Encryption	Module initialization
AES-ECB - Encrypt (A5508)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Encryption	Module initialization
AES-ECB - Encrypt (A5509)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Encryption	Module initialization
AES-ECB - Encrypt (A5510)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Encryption	Module initialization
AES-ECB - Encrypt (A5511)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Encryption	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-ECB - Encrypt (A5512)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Encryption	Module initialization
AES-ECB - Encrypt (A5513)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Encryption	Module initialization
AES-ECB - Encrypt (A5514)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Encryption	Module initialization
AES-ECB - Encrypt (A5515)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Encryption	Module initialization
AES-ECB - Encrypt (A5520)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Encryption	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-ECB - Encrypt (A5521)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Encryption	Module initialization
AES-ECB - Encrypt (A5522)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Encryption	Module initialization
AES-ECB - Encrypt (A5523)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Encryption	Module initialization
AES-ECB - Encrypt (A5524)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Encryption	Module initialization
AES-ECB - Encrypt (A5526)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Encryption	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-ECB - Encrypt (A5528)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Encryption	Module initialization
AES-ECB - Encrypt (A5529)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Encryption	Module initialization
AES-ECB - Encrypt (A5530)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Encryption	Module initialization
AES-ECB - Encrypt (A5531)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Encryption	Module initialization
AES-ECB - Encrypt (A5532)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Encryption	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-ECB - Encrypt (A5533)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Encryption	Module initialization
AES-ECB - Encrypt (A5534)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Encryption	Module initialization
AES-ECB - Encrypt (A5535)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Encryption	Module initialization
AES-ECB - Encrypt (A5536)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Encryption	Module initialization
AES-ECB - Encrypt (A5537)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Encryption	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-ECB - Encrypt (A5538)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Encryption	Module initialization
AES-ECB - Encrypt (A5661)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Encryption	Module initialization
AES-ECB - Encrypt (A5662)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Encryption	Module initialization
AES-ECB - Encrypt (A5663)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Encryption	Module initialization
AES-ECB - Encrypt (A5664)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Encryption	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-ECB - Encrypt (A5665)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Encryption	Module initialization
AES-ECB - Encrypt (A5666)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Encryption	Module initialization
AES-ECB - Decrypt (A5503)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Decryption	Module initialization
AES-ECB - Decrypt (A5505)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Decryption	Module initialization
AES-ECB - Decrypt (A5506)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Decryption	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-ECB - Decrypt (A5507)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Decryption	Module initialization
AES-ECB - Decrypt (A5508)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Decryption	Module initialization
AES-ECB - Decrypt (A5509)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Decryption	Module initialization
AES-ECB - Decrypt (A5510)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Decryption	Module initialization
AES-ECB - Decrypt (A5511)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Decryption	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-ECB - Decrypt (A5512)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Decryption	Module initialization
AES-ECB - Decrypt (A5513)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Decryption	Module initialization
AES-ECB - Decrypt (A5514)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Decryption	Module initialization
AES-ECB - Decrypt (A5515)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Decryption	Module initialization
AES-ECB - Decrypt (A5520)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Decryption	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-ECB - Decrypt (A5521)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Decryption	Module initialization
AES-ECB - Decrypt (A5522)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Decryption	Module initialization
AES-ECB - Decrypt (A5523)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Decryption	Module initialization
AES-ECB - Decrypt (A5524)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Decryption	Module initialization
AES-ECB - Decrypt (A5526)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Decryption	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-ECB - Decrypt (A5528)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Decryption	Module initialization
AES-ECB - Decrypt (A5529)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Decryption	Module initialization
AES-ECB - Decrypt (A5530)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Decryption	Module initialization
AES-ECB - Decrypt (A5531)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Decryption	Module initialization
AES-ECB - Decrypt (A5532)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Decryption	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-ECB - Decrypt (A5533)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Decryption	Module initialization
AES-ECB - Decrypt (A5534)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Decryption	Module initialization
AES-ECB - Decrypt (A5535)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Decryption	Module initialization
AES-ECB - Decrypt (A5536)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Decryption	Module initialization
AES-ECB - Decrypt (A5537)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Decryption	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-ECB - Decrypt (A5538)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Decryption	Module initialization
AES-ECB - Decrypt (A5661)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Decryption	Module initialization
AES-ECB - Decrypt (A5662)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Decryption	Module initialization
AES-ECB - Decrypt (A5663)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Decryption	Module initialization
AES-ECB - Decrypt (A5664)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Decryption	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-ECB - Decrypt (A5665)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Decryption	Module initialization
AES-ECB - Decrypt (A5666)	128, 192, 256 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Decryption	Module initialization
HMAC-SHA-1 (A5503)	32-64 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
HMAC-SHA-1 (A5516)	32-64 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
HMAC-SHA-1 (A5517)	32-64 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HMAC-SHA-1 (A5518)	32-64 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
HMAC-SHA-1 (A5519)	32-64 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
HMAC-SHA-1 (A5520)	32-64 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
HMAC-SHA-1 (A5526)	32-64 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
HMAC-SHA-1 (A5539)	32-64 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HMAC-SHA-1 (A5540)	32-64 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
HMAC-SHA-1 (A5541)	32-64 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
HMAC-SHA-1 (A5542)	32-64 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
HMAC-SHA-1 (A5664)	32-64 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
HMAC-SHA2-224 (A5503)	32-1048 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HMAC-SHA2-224 (A5516)	32-1048 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
HMAC-SHA2-224 (A5517)	32-1048 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
HMAC-SHA2-224 (A5518)	32-1048 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
HMAC-SHA2-224 (A5519)	32-1048 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
HMAC-SHA2-224 (A5520)	32-1048 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HMAC-SHA2-224 (A5524)	32-1048 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
HMAC-SHA2-224 (A5525)	32-1048 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
HMAC-SHA2-224 (A5526)	32-1048 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
HMAC-SHA2-224 (A5539)	32-1048 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
HMAC-SHA2-224 (A5540)	32-1048 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HMAC-SHA2-224 (A5541)	32-1048 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
HMAC-SHA2-224 (A5542)	32-1048 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
HMAC-SHA2-224 (A5664)	32-1048 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
HMAC-SHA2-256 (A5503)	32-64 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization. Before integrity test.
HMAC-SHA2-256 (A5516)	32-64 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization. Before integrity test.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HMAC-SHA2-256 (A5517)	32-64 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization. Before integrity test.
HMAC-SHA2-256 (A5518)	32-64 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization. Before integrity test.
HMAC-SHA2-256 (A5519)	32-64 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization. Before integrity test.
HMAC-SHA2-256 (A5520)	32-64 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization. Before integrity test.
HMAC-SHA2-256 (A5524)	32-64 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization. Before integrity test.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HMAC-SHA2-256 (A5525)	32-64 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization. Before integrity test.
HMAC-SHA2-256 (A5526)	32-64 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization. Before integrity test.
HMAC-SHA2-256 (A5539)	32-64 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization. Before integrity test.
HMAC-SHA2-256 (A5540)	32-64 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization. Before integrity test.
HMAC-SHA2-256 (A5541)	32-64 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization. Before integrity test.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HMAC-SHA2-256 (A5542)	32-64 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization. Before integrity test.
HMAC-SHA2-256 (A5664)	32-64 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization. Before integrity test.
HMAC-SHA2-384 (A5503)	32-1048 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
HMAC-SHA2-384 (A5516)	32-1048 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
HMAC-SHA2-384 (A5517)	32-1048 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HMAC-SHA2-384 (A5518)	32-1048 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
HMAC-SHA2-384 (A5525)	32-1048 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
HMAC-SHA2-384 (A5526)	32-1048 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
HMAC-SHA2-384 (A5539)	32-1048 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
HMAC-SHA2-384 (A5540)	32-1048 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HMAC-SHA2-384 (A5541)	32-1048 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
HMAC-SHA2-384 (A5664)	32-1048 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
HMAC-SHA2-512 (A5503)	32-1048 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization. Before integrity test.
HMAC-SHA2-512 (A5516)	32-1048 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization. Before integrity test.
HMAC-SHA2-512 (A5517)	32-1048 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization. Before integrity test.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HMAC-SHA2-512 (A5518)	32-1048 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization. Before integrity test.
HMAC-SHA2-512 (A5525)	32-1048 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization. Before integrity test.
HMAC-SHA2-512 (A5526)	32-1048 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization. Before integrity test.
HMAC-SHA2-512 (A5539)	32-1048 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization. Before integrity test.
HMAC-SHA2-512 (A5540)	32-1048 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization. Before integrity test.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HMAC-SHA2-512 (A5541)	32-1048 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization. Before integrity test.
HMAC-SHA2-512 (A5664)	32-1048 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization. Before integrity test.
HMAC-SHA3-224 (A5503)	32-1048 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
HMAC-SHA3-224 (A5526)	32-1048 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
HMAC-SHA3-224 (A5664)	32-1048 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HMAC-SHA3-256 (A5503)	32-1048 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
HMAC-SHA3-256 (A5526)	32-1048 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
HMAC-SHA3-256 (A5664)	32-1048 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
HMAC-SHA3-384 (A5503)	32-1048 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
HMAC-SHA3-384 (A5526)	32-1048 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HMAC-SHA3-384 (A5664)	32-1048 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
HMAC-SHA3-512 (A5503)	32-1048 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
HMAC-SHA3-512 (A5526)	32-1048 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
HMAC-SHA3-512 (A5664)	32-1048 bit keys	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Module initialization
Counter DRBG (A5503)	128, 192, 256 bit keys with DF, with/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Instantiate, Reseed, Generate	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
Counter DRBG (A5505)	128, 192, 256 bit keys with DF, with/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Instantiate, Reseed, Generate	Module initialization
Counter DRBG (A5506)	128, 192, 256 bit keys with DF, with/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Instantiate, Reseed, Generate	Module initialization
Counter DRBG (A5507)	128, 192, 256 bit keys with DF, with/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Instantiate, Reseed, Generate	Module initialization
Counter DRBG (A5508)	128, 192, 256 bit keys with DF, with/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Instantiate, Reseed, Generate	Module initialization
Counter DRBG (A5509)	128, 192, 256 bit keys with DF, with/without PR; Health test per section 11.3	KAT	CAST	Module becomes operational and services are	Instantiate, Reseed, Generate	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
	of SP 800-90Arev1			available for use.		
Counter DRBG (A5510)	128, 192, 256 bit keys with DF, with/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Instantiate, Reseed, Generate	Module initialization
Counter DRBG (A5511)	128, 192, 256 bit keys with DF, with/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Instantiate, Reseed, Generate	Module initialization
Counter DRBG (A5512)	128, 192, 256 bit keys with DF, with/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Instantiate, Reseed, Generate	Module initialization
Counter DRBG (A5513)	128, 192, 256 bit keys with DF, with/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Instantiate, Reseed, Generate	Module initialization
Counter DRBG (A5514)	128, 192, 256 bit keys with DF, with/without PR; Health	KAT	CAST	Module becomes operational and services	Instantiate, Reseed, Generate	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
	test per section 11.3 of SP 800-90Arev1			are available for use.		
Counter DRBG (A5515)	128, 192, 256 bit keys with DF, with/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Instantiate, Reseed, Generate	Module initialization
Counter DRBG (A5521)	128, 192, 256 bit keys with DF, with/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Instantiate, Reseed, Generate	Module initialization
Counter DRBG (A5522)	128, 192, 256 bit keys with DF, with/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Instantiate, Reseed, Generate	Module initialization
Counter DRBG (A5523)	128, 192, 256 bit keys with DF, with/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Instantiate, Reseed, Generate	Module initialization
Counter DRBG (A5526)	128, 192, 256 bit keys with DF,	KAT	CAST	Module becomes operationa	Instantiate, Reseed, Generate	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
	with/without PR; Health test per section 11.3 of SP 800-90Arev1			l and services are available for use.		
Counter DRBG (A5528)	128, 192, 256 bit keys with DF, with/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Instantiate, Reseed, Generate	Module initialization
Counter DRBG (A5529)	128, 192, 256 bit keys with DF, with/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Instantiate, Reseed, Generate	Module initialization
Counter DRBG (A5530)	128, 192, 256 bit keys with DF, with/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Instantiate, Reseed, Generate	Module initialization
Counter DRBG (A5531)	128, 192, 256 bit keys with DF, with/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Instantiate, Reseed, Generate	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
Counter DRBG (A5532)	128, 192, 256 bit keys with DF, with/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Instantiate, Reseed, Generate	Module initialization
Counter DRBG (A5533)	128, 192, 256 bit keys with DF, with/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Instantiate, Reseed, Generate	Module initialization
Counter DRBG (A5534)	128, 192, 256 bit keys with DF, with/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Instantiate, Reseed, Generate	Module initialization
Counter DRBG (A5535)	128, 192, 256 bit keys with DF, with/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Instantiate, Reseed, Generate	Module initialization
Counter DRBG (A5536)	128, 192, 256 bit keys with DF, with/without PR; Health test per section 11.3	KAT	CAST	Module becomes operational and services are	Instantiate, Reseed, Generate	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
	of SP 800-90Arev1			available for use.		
Counter DRBG (A5537)	128, 192, 256 bit keys with DF, with/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Instantiate, Reseed, Generate	Module initialization
Counter DRBG (A5538)	128, 192, 256 bit keys with DF, with/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Instantiate, Reseed, Generate	Module initialization
Counter DRBG (A5661)	128, 192, 256 bit keys with DF, with/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Instantiate, Reseed, Generate	Module initialization
Counter DRBG (A5662)	128, 192, 256 bit keys with DF, with/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Instantiate, Reseed, Generate	Module initialization
Counter DRBG (A5663)	128, 192, 256 bit keys with DF, with/without PR; Health	KAT	CAST	Module becomes operational and services	Instantiate, Reseed, Generate	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
	test per section 11.3 of SP 800-90Arev1			are available for use.		
Counter DRBG (A5664)	128, 192, 256 bit keys with DF, with/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Instantiate, Reseed, Generate	Module initialization
Counter DRBG (A5665)	128, 192, 256 bit keys with DF, with/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Instantiate, Reseed, Generate	Module initialization
Counter DRBG (A5666)	128, 192, 256 bit keys with DF, with/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Instantiate, Reseed, Generate	Module initialization
Hash DRBG (A5503)	SHA2-256 With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Instantiate, Reseed, Generate	Module initialization
Hash DRBG (A5516)	SHA2-256 With/without PR; Health test per	KAT	CAST	Module becomes operational and	Instantiate, Reseed, Generate	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
	section 11.3 of SP 800-90Arev1			services are available for use.		
Hash DRBG (A5517)	SHA2-256 With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Instantiate, Reseed, Generate	Module initialization
Hash DRBG (A5518)	SHA2-256 With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Instantiate, Reseed, Generate	Module initialization
Hash DRBG (A5526)	SHA2-256 With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Instantiate, Reseed, Generate	Module initialization
Hash DRBG (A5539)	SHA2-256 With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Instantiate, Reseed, Generate	Module initialization
Hash DRBG (A5540)	SHA2-256 With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are	Instantiate, Reseed, Generate	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				available for use.		
Hash DRBG (A5541)	SHA2-256 With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Instantiate, Reseed, Generate	Module initialization
Hash DRBG (A5664)	SHA2-256 With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Instantiate, Reseed, Generate	Module initialization
HMAC DRBG (A5503)	SHA2-256, SHA2-512 With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Instantiate, Reseed, Generate	Module initialization
HMAC DRBG (A5516)	SHA2-256, SHA2-512 With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Instantiate, Reseed, Generate	Module initialization
HMAC DRBG (A5517)	SHA2-256, SHA2-512 With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Instantiate, Reseed, Generate	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HMAC DRBG (A5518)	SHA2-256, SHA2-512 With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Instantiate, Reseed, Generate	Module initialization
HMAC DRBG (A5526)	SHA2-256, SHA2-512 With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Instantiate, Reseed, Generate	Module initialization
HMAC DRBG (A5539)	SHA2-256, SHA2-512 With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Instantiate, Reseed, Generate	Module initialization
HMAC DRBG (A5540)	SHA2-256, SHA2-512 With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Instantiate, Reseed, Generate	Module initialization
HMAC DRBG (A5541)	SHA2-256, SHA2-512 With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Instantiate, Reseed, Generate	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HMAC DRBG (A5664)	SHA2-256, SHA2-512 With/without PR; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module becomes operational and services are available for use.	Instantiate, Reseed, Generate	Module initialization
ECDSA SigVer (FIPS186-5) (A5504)	P-256 with SHA-256	KAT	CAST	Module becomes operational and services are available for use.	Verify	Module initialization
ECDSA SigVer (FIPS186-5) (A5527)	P-256 with SHA-256	KAT	CAST	Module becomes operational and services are available for use.	Verify	Module initialization
RSA SigVer (FIPS186-5) (A5503)	4096-bit key with SHA-256	KAT	CAST	Module becomes operational and services are available for use.	Verify	Module initialization. Before integrity test.
RSA SigVer (FIPS186-5) (A5526)	4096-bit key with SHA-256	KAT	CAST	Module becomes operational and services are available for use.	Verify	Module initialization. Before integrity test.
RSA SigVer	4096-bit key with SHA-256	KAT	CAST	Module becomes operationa	Verify	Module initialization.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
(FIPS186-5) (A5664)				l and services are available for use.		Before integrity test.
KDF SP800-108 (A5503)	512 bit key-derivation key with hmac(sha256) deriving a 256 bits of key material	KAT	CAST	Module becomes operational and services are available for use.	Derivation	Module initialization
KDF SP800-108 (A5526)	512 bit key-derivation key with hmac(sha256) deriving a 256 bits of key material	KAT	CAST	Module becomes operational and services are available for use.	Derivation	Module initialization
KAS-ECC-SSC Sp800-56Ar3 (A5503)	P-256 and P-384	KAT	CAST	Module becomes operational and services are available for use.	Shared secret computation	Module initialization
KAS-ECC-SSC Sp800-56Ar3 (A5526)	P-256 and P-384	KAT	CAST	Module becomes operational and services are available for use.	Shared secret computation	Module initialization
KAS-FFC-SSC Sp800-56Ar3 (A5503)	ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, and ffdhe8192	KAT	CAST	Module becomes operational and services are	Shared secret computation	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				available for use.		
KAS-FFC-SSC Sp800-56Ar3 (A5526)	ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, and ffdhe8192	KAT	CAST	Module becomes operational and services are available for use.	Shared secret computation	Module initialization
ECDSA KeyGen (FIPS186-5) (A5503)	PCT according to Section 5.6.2.1.4 of SP 800-56A Rev. 3	PCT	PCT	Module becomes operational and services are available for use.	Public key recomputation	During operational state of the module when the respective cryptographic functions are used.
ECDSA KeyGen (FIPS186-5) (A5526)	PCT according to Section 5.6.2.1.4 of SP 800-56A Rev. 3	PCT	PCT	Module becomes operational and services are available for use.	Public key recomputation	During operational state of the module when the respective cryptographic functions are used.
Safe Primes Key Generation (A5503)	PCT according to Section 5.6.2.1.4 of SP 800-56A Rev. 3	PCT	PCT	Module becomes operational and services are available for use.	Public key recomputation	During operational state of the module when the respective cryptographic functions are used.
Safe Primes Key Generation (A5526)	PCT according to Section 5.6.2.1.4 of SP 800-56A Rev. 3	PCT	PCT	Module becomes operational and services are	Public key recomputation	During operational state of the module when the respective

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				available for use.		cryptographic functions are used.
Entropy Source - RCT start-up test	Cutoff C=61, 1024 samples. Repetition count test according to Section 4.4.1 of SP 800-90B	RCT	CAST	Module becomes operational and services are available for use.	Entropy source start-up test	Entropy source initialization
Entropy Source - APT start-up test	Cutoff C=355, window W=512, 1024 samples. Adaptive proportion test according to Section 4.4.2 of SP 800-90B	APT	CAST	Module becomes operational and services are available for use.	Entropy source start-up test	Entropy source initialization
Entropy Source - RCT continuous test	Intermittent cutoff C=31, permanent cutoff C=61. Repetition count test according to Section 4.4.1 of SP 800-90B	RCT	CAST	Entropy source is operational and services are available for use.	Entropy source continuous test	Continuously when the entropy source is accessed
Entropy Source - APT continuous test	Intermittent cutoff C=325, permanent cutoff C=255, window W=512. Adaptive proportion test according to Section 4.4.2 of SP 800-90B	APT	CAST	Entropy source is operational and services are available for use.	Entropy source continuous test	Continuously when the entropy source is accessed

Table 22: Conditional Self-Tests

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

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
HMAC-SHA2-256 (A5503) - kernel version 3.5	Message Authentication	SW/FW Integrity	On demand	Manually
HMAC-SHA2-256 (A5503) - fipscheck version 3.5	Message Authentication	SW/FW Integrity	On demand	Manually
RSA SigVer (FIPS186-5) (A5503) - object files version 3.5	Signature Verification	SW/FW Integrity	On demand	Manually
HMAC-SHA2-256 (A5526) - kernel version 3.6	Message Authentication	SW/FW Integrity	On demand	Manually
HMAC-SHA2-256 (A5526) - fipscheck version 3.6	Message Authentication	SW/FW Integrity	On demand	Manually
RSA SigVer (FIPS186-5) (A5526) - object files version 3.6	Signature Verification	SW/FW Integrity	On demand	Manually

Table 23: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
SHA-1 (A5503)	KAT	CAST	On demand	Manually
SHA-1 (A5516)	KAT	CAST	On demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
SHA-1 (A5517)	KAT	CAST	On demand	Manually
SHA-1 (A5518)	KAT	CAST	On demand	Manually
SHA-1 (A5519)	KAT	CAST	On demand	Manually
SHA-1 (A5520)	KAT	CAST	On demand	Manually
SHA-1 (A5526)	KAT	CAST	On demand	Manually
SHA-1 (A5539)	KAT	CAST	On demand	Manually
SHA-1 (A5540)	KAT	CAST	On demand	Manually
SHA-1 (A5541)	KAT	CAST	On demand	Manually
SHA-1 (A5542)	KAT	CAST	On demand	Manually
SHA-1 (A5664)	KAT	CAST	On demand	Manually
SHA2-256 (A5503)	KAT	CAST	On demand	Manually
SHA2-256 (A5516)	KAT	CAST	On demand	Manually
SHA2-256 (A5517)	KAT	CAST	On demand	Manually
SHA2-256 (A5518)	KAT	CAST	On demand	Manually
SHA2-256 (A5519)	KAT	CAST	On demand	Manually
SHA2-256 (A5520)	KAT	CAST	On demand	Manually
SHA2-256 (A5524)	KAT	CAST	On demand	Manually
SHA2-256 (A5525)	KAT	CAST	On demand	Manually
SHA2-256 (A5526)	KAT	CAST	On demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
SHA2-256 (A5539)	KAT	CAST	On demand	Manually
SHA2-256 (A5540)	KAT	CAST	On demand	Manually
SHA2-256 (A5541)	KAT	CAST	On demand	Manually
SHA2-256 (A5542)	KAT	CAST	On demand	Manually
SHA2-256 (A5664)	KAT	CAST	On demand	Manually
SHA2-512 (A5503)	KAT	CAST	On demand	Manually
SHA2-512 (A5516)	KAT	CAST	On demand	Manually
SHA2-512 (A5517)	KAT	CAST	On demand	Manually
SHA2-512 (A5518)	KAT	CAST	On demand	Manually
SHA2-512 (A5525)	KAT	CAST	On demand	Manually
SHA2-512 (A5526)	KAT	CAST	On demand	Manually
SHA2-512 (A5539)	KAT	CAST	On demand	Manually
SHA2-512 (A5540)	KAT	CAST	On demand	Manually
SHA2-512 (A5541)	KAT	CAST	On demand	Manually
SHA2-512 (A5664)	KAT	CAST	On demand	Manually
SHA3-224 (A5503)	KAT	CAST	On demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
SHA3-224 (A5526)	KAT	CAST	On demand	Manually
SHA3-224 (A5664)	KAT	CAST	On demand	Manually
SHA3-256 (A5503)	KAT	CAST	On demand	Manually
SHA3-256 (A5526)	KAT	CAST	On demand	Manually
SHA3-256 (A5664)	KAT	CAST	On demand	Manually
SHA3-384 (A5503)	KAT	CAST	On demand	Manually
SHA3-384 (A5526)	KAT	CAST	On demand	Manually
SHA3-384 (A5664)	KAT	CAST	On demand	Manually
SHA3-512 (A5503)	KAT	CAST	On demand	Manually
SHA3-512 (A5526)	KAT	CAST	On demand	Manually
SHA3-512 (A5664)	KAT	CAST	On demand	Manually
AES-GCM - Encrypt (A5503)	KAT	CAST	On demand	Manually
AES-GCM - Encrypt (A5505)	KAT	CAST	On demand	Manually
AES-GCM - Encrypt (A5506)	KAT	CAST	On demand	Manually
AES-GCM - Encrypt (A5507)	KAT	CAST	On demand	Manually
AES-GCM - Encrypt (A5508)	KAT	CAST	On demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-GCM - Encrypt (A5509)	KAT	CAST	On demand	Manually
AES-GCM - Encrypt (A5510)	KAT	CAST	On demand	Manually
AES-GCM - Encrypt (A5511)	KAT	CAST	On demand	Manually
AES-GCM - Encrypt (A5512)	KAT	CAST	On demand	Manually
AES-GCM - Encrypt (A5513)	KAT	CAST	On demand	Manually
AES-GCM - Encrypt (A5514)	KAT	CAST	On demand	Manually
AES-GCM - Encrypt (A5515)	KAT	CAST	On demand	Manually
AES-GCM - Encrypt (A5521)	KAT	CAST	On demand	Manually
AES-GCM - Encrypt (A5522)	KAT	CAST	On demand	Manually
AES-GCM - Encrypt (A5523)	KAT	CAST	On demand	Manually
AES-GCM - Encrypt (A5526)	KAT	CAST	On demand	Manually
AES-GCM - Encrypt (A5528)	KAT	CAST	On demand	Manually
AES-GCM - Encrypt (A5529)	KAT	CAST	On demand	Manually
AES-GCM - Encrypt (A5530)	KAT	CAST	On demand	Manually
AES-GCM - Encrypt (A5531)	KAT	CAST	On demand	Manually
AES-GCM - Encrypt (A5532)	KAT	CAST	On demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-GCM - Encrypt (A5533)	KAT	CAST	On demand	Manually
AES-GCM - Encrypt (A5534)	KAT	CAST	On demand	Manually
AES-GCM - Encrypt (A5535)	KAT	CAST	On demand	Manually
AES-GCM - Encrypt (A5536)	KAT	CAST	On demand	Manually
AES-GCM - Encrypt (A5537)	KAT	CAST	On demand	Manually
AES-GCM - Encrypt (A5538)	KAT	CAST	On demand	Manually
AES-GCM - Encrypt (A5661)	KAT	CAST	On demand	Manually
AES-GCM - Encrypt (A5662)	KAT	CAST	On demand	Manually
AES-GCM - Encrypt (A5663)	KAT	CAST	On demand	Manually
AES-GCM - Encrypt (A5664)	KAT	CAST	On demand	Manually
AES-GCM - Encrypt (A5665)	KAT	CAST	On demand	Manually
AES-GCM - Encrypt (A5666)	KAT	CAST	On demand	Manually
AES-GCM - Decrypt (A5503)	KAT	CAST	On demand	Manually
AES-GCM - Decrypt (A5505)	KAT	CAST	On demand	Manually
AES-GCM - Decrypt (A5506)	KAT	CAST	On demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-GCM - Decrypt (A5507)	KAT	CAST	On demand	Manually
AES-GCM - Decrypt (A5508)	KAT	CAST	On demand	Manually
AES-GCM - Decrypt (A5509)	KAT	CAST	On demand	Manually
AES-GCM - Decrypt (A5510)	KAT	CAST	On demand	Manually
AES-GCM - Decrypt (A5511)	KAT	CAST	On demand	Manually
AES-GCM - Decrypt (A5512)	KAT	CAST	On demand	Manually
AES-GCM - Decrypt (A5513)	KAT	CAST	On demand	Manually
AES-GCM - Decrypt (A5514)	KAT	CAST	On demand	Manually
AES-GCM - Decrypt (A5515)	KAT	CAST	On demand	Manually
AES-GCM - Decrypt (A5521)	KAT	CAST	On demand	Manually
AES-GCM - Decrypt (A5522)	KAT	CAST	On demand	Manually
AES-GCM - Decrypt (A5523)	KAT	CAST	On demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-GCM - Decrypt (A5526)	KAT	CAST	On demand	Manually
AES-GCM - Decrypt (A5528)	KAT	CAST	On demand	Manually
AES-GCM - Decrypt (A5529)	KAT	CAST	On demand	Manually
AES-GCM - Decrypt (A5530)	KAT	CAST	On demand	Manually
AES-GCM - Decrypt (A5531)	KAT	CAST	On demand	Manually
AES-GCM - Decrypt (A5532)	KAT	CAST	On demand	Manually
AES-GCM - Decrypt (A5533)	KAT	CAST	On demand	Manually
AES-GCM - Decrypt (A5534)	KAT	CAST	On demand	Manually
AES-GCM - Decrypt (A5535)	KAT	CAST	On demand	Manually
AES-GCM - Decrypt (A5536)	KAT	CAST	On demand	Manually
AES-GCM - Decrypt (A5537)	KAT	CAST	On demand	Manually
AES-GCM - Decrypt (A5538)	KAT	CAST	On demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-GCM - Decrypt (A5661)	KAT	CAST	On demand	Manually
AES-GCM - Decrypt (A5662)	KAT	CAST	On demand	Manually
AES-GCM - Decrypt (A5663)	KAT	CAST	On demand	Manually
AES-GCM - Decrypt (A5664)	KAT	CAST	On demand	Manually
AES-GCM - Decrypt (A5665)	KAT	CAST	On demand	Manually
AES-GCM - Decrypt (A5666)	KAT	CAST	On demand	Manually
AES-ECB - Encrypt (A5503)	KAT	CAST	On demand	Manually
AES-ECB - Encrypt (A5505)	KAT	CAST	On demand	Manually
AES-ECB - Encrypt (A5506)	KAT	CAST	On demand	Manually
AES-ECB - Encrypt (A5507)	KAT	CAST	On demand	Manually
AES-ECB - Encrypt (A5508)	KAT	CAST	On demand	Manually
AES-ECB - Encrypt (A5509)	KAT	CAST	On demand	Manually
AES-ECB - Encrypt (A5510)	KAT	CAST	On demand	Manually
AES-ECB - Encrypt (A5511)	KAT	CAST	On demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-ECB - Encrypt (A5512)	KAT	CAST	On demand	Manually
AES-ECB - Encrypt (A5513)	KAT	CAST	On demand	Manually
AES-ECB - Encrypt (A5514)	KAT	CAST	On demand	Manually
AES-ECB - Encrypt (A5515)	KAT	CAST	On demand	Manually
AES-ECB - Encrypt (A5520)	KAT	CAST	On demand	Manually
AES-ECB - Encrypt (A5521)	KAT	CAST	On demand	Manually
AES-ECB - Encrypt (A5522)	KAT	CAST	On demand	Manually
AES-ECB - Encrypt (A5523)	KAT	CAST	On demand	Manually
AES-ECB - Encrypt (A5524)	KAT	CAST	On demand	Manually
AES-ECB - Encrypt (A5526)	KAT	CAST	On demand	Manually
AES-ECB - Encrypt (A5528)	KAT	CAST	On demand	Manually
AES-ECB - Encrypt (A5529)	KAT	CAST	On demand	Manually
AES-ECB - Encrypt (A5530)	KAT	CAST	On demand	Manually
AES-ECB - Encrypt (A5531)	KAT	CAST	On demand	Manually
AES-ECB - Encrypt (A5532)	KAT	CAST	On demand	Manually
AES-ECB - Encrypt (A5533)	KAT	CAST	On demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-ECB - Encrypt (A5534)	KAT	CAST	On demand	Manually
AES-ECB - Encrypt (A5535)	KAT	CAST	On demand	Manually
AES-ECB - Encrypt (A5536)	KAT	CAST	On demand	Manually
AES-ECB - Encrypt (A5537)	KAT	CAST	On demand	Manually
AES-ECB - Encrypt (A5538)	KAT	CAST	On demand	Manually
AES-ECB - Encrypt (A5661)	KAT	CAST	On demand	Manually
AES-ECB - Encrypt (A5662)	KAT	CAST	On demand	Manually
AES-ECB - Encrypt (A5663)	KAT	CAST	On demand	Manually
AES-ECB - Encrypt (A5664)	KAT	CAST	On demand	Manually
AES-ECB - Encrypt (A5665)	KAT	CAST	On demand	Manually
AES-ECB - Encrypt (A5666)	KAT	CAST	On demand	Manually
AES-ECB - Decrypt (A5503)	KAT	CAST	On demand	Manually
AES-ECB - Decrypt (A5505)	KAT	CAST	On demand	Manually
AES-ECB - Decrypt (A5506)	KAT	CAST	On demand	Manually
AES-ECB - Decrypt (A5507)	KAT	CAST	On demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-ECB - Decrypt (A5508)	KAT	CAST	On demand	Manually
AES-ECB - Decrypt (A5509)	KAT	CAST	On demand	Manually
AES-ECB - Decrypt (A5510)	KAT	CAST	On demand	Manually
AES-ECB - Decrypt (A5511)	KAT	CAST	On demand	Manually
AES-ECB - Decrypt (A5512)	KAT	CAST	On demand	Manually
AES-ECB - Decrypt (A5513)	KAT	CAST	On demand	Manually
AES-ECB - Decrypt (A5514)	KAT	CAST	On demand	Manually
AES-ECB - Decrypt (A5515)	KAT	CAST	On demand	Manually
AES-ECB - Decrypt (A5520)	KAT	CAST	On demand	Manually
AES-ECB - Decrypt (A5521)	KAT	CAST	On demand	Manually
AES-ECB - Decrypt (A5522)	KAT	CAST	On demand	Manually
AES-ECB - Decrypt (A5523)	KAT	CAST	On demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-ECB - Decrypt (A5524)	KAT	CAST	On demand	Manually
AES-ECB - Decrypt (A5526)	KAT	CAST	On demand	Manually
AES-ECB - Decrypt (A5528)	KAT	CAST	On demand	Manually
AES-ECB - Decrypt (A5529)	KAT	CAST	On demand	Manually
AES-ECB - Decrypt (A5530)	KAT	CAST	On demand	Manually
AES-ECB - Decrypt (A5531)	KAT	CAST	On demand	Manually
AES-ECB - Decrypt (A5532)	KAT	CAST	On demand	Manually
AES-ECB - Decrypt (A5533)	KAT	CAST	On demand	Manually
AES-ECB - Decrypt (A5534)	KAT	CAST	On demand	Manually
AES-ECB - Decrypt (A5535)	KAT	CAST	On demand	Manually
AES-ECB - Decrypt (A5536)	KAT	CAST	On demand	Manually
AES-ECB - Decrypt (A5537)	KAT	CAST	On demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-ECB - Decrypt (A5538)	KAT	CAST	On demand	Manually
AES-ECB - Decrypt (A5661)	KAT	CAST	On demand	Manually
AES-ECB - Decrypt (A5662)	KAT	CAST	On demand	Manually
AES-ECB - Decrypt (A5663)	KAT	CAST	On demand	Manually
AES-ECB - Decrypt (A5664)	KAT	CAST	On demand	Manually
AES-ECB - Decrypt (A5665)	KAT	CAST	On demand	Manually
AES-ECB - Decrypt (A5666)	KAT	CAST	On demand	Manually
HMAC-SHA-1 (A5503)	KAT	CAST	On demand	Manually
HMAC-SHA-1 (A5516)	KAT	CAST	On demand	Manually
HMAC-SHA-1 (A5517)	KAT	CAST	On demand	Manually
HMAC-SHA-1 (A5518)	KAT	CAST	On demand	Manually
HMAC-SHA-1 (A5519)	KAT	CAST	On demand	Manually
HMAC-SHA-1 (A5520)	KAT	CAST	On demand	Manually
HMAC-SHA-1 (A5526)	KAT	CAST	On demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
HMAC-SHA-1 (A5539)	KAT	CAST	On demand	Manually
HMAC-SHA-1 (A5540)	KAT	CAST	On demand	Manually
HMAC-SHA-1 (A5541)	KAT	CAST	On demand	Manually
HMAC-SHA-1 (A5542)	KAT	CAST	On demand	Manually
HMAC-SHA-1 (A5664)	KAT	CAST	On demand	Manually
HMAC-SHA2-224 (A5503)	KAT	CAST	On demand	Manually
HMAC-SHA2-224 (A5516)	KAT	CAST	On demand	Manually
HMAC-SHA2-224 (A5517)	KAT	CAST	On demand	Manually
HMAC-SHA2-224 (A5518)	KAT	CAST	On demand	Manually
HMAC-SHA2-224 (A5519)	KAT	CAST	On demand	Manually
HMAC-SHA2-224 (A5520)	KAT	CAST	On demand	Manually
HMAC-SHA2-224 (A5524)	KAT	CAST	On demand	Manually
HMAC-SHA2-224 (A5525)	KAT	CAST	On demand	Manually
HMAC-SHA2-224 (A5526)	KAT	CAST	On demand	Manually
HMAC-SHA2-224 (A5539)	KAT	CAST	On demand	Manually
HMAC-SHA2-224 (A5540)	KAT	CAST	On demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
HMAC-SHA2-224 (A5541)	KAT	CAST	On demand	Manually
HMAC-SHA2-224 (A5542)	KAT	CAST	On demand	Manually
HMAC-SHA2-224 (A5664)	KAT	CAST	On demand	Manually
HMAC-SHA2-256 (A5503)	KAT	CAST	On demand	Manually
HMAC-SHA2-256 (A5516)	KAT	CAST	On demand	Manually
HMAC-SHA2-256 (A5517)	KAT	CAST	On demand	Manually
HMAC-SHA2-256 (A5518)	KAT	CAST	On demand	Manually
HMAC-SHA2-256 (A5519)	KAT	CAST	On demand	Manually
HMAC-SHA2-256 (A5520)	KAT	CAST	On demand	Manually
HMAC-SHA2-256 (A5524)	KAT	CAST	On demand	Manually
HMAC-SHA2-256 (A5525)	KAT	CAST	On demand	Manually
HMAC-SHA2-256 (A5526)	KAT	CAST	On demand	Manually
HMAC-SHA2-256 (A5539)	KAT	CAST	On demand	Manually
HMAC-SHA2-256 (A5540)	KAT	CAST	On demand	Manually
HMAC-SHA2-256 (A5541)	KAT	CAST	On demand	Manually
HMAC-SHA2-256 (A5542)	KAT	CAST	On demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
HMAC-SHA2-256 (A5664)	KAT	CAST	On demand	Manually
HMAC-SHA2-384 (A5503)	KAT	CAST	On demand	Manually
HMAC-SHA2-384 (A5516)	KAT	CAST	On demand	Manually
HMAC-SHA2-384 (A5517)	KAT	CAST	On demand	Manually
HMAC-SHA2-384 (A5518)	KAT	CAST	On demand	Manually
HMAC-SHA2-384 (A5525)	KAT	CAST	On demand	Manually
HMAC-SHA2-384 (A5526)	KAT	CAST	On demand	Manually
HMAC-SHA2-384 (A5539)	KAT	CAST	On demand	Manually
HMAC-SHA2-384 (A5540)	KAT	CAST	On demand	Manually
HMAC-SHA2-384 (A5541)	KAT	CAST	On demand	Manually
HMAC-SHA2-384 (A5664)	KAT	CAST	On demand	Manually
HMAC-SHA2-512 (A5503)	KAT	CAST	On demand	Manually
HMAC-SHA2-512 (A5516)	KAT	CAST	On demand	Manually
HMAC-SHA2-512 (A5517)	KAT	CAST	On demand	Manually
HMAC-SHA2-512 (A5518)	KAT	CAST	On demand	Manually
HMAC-SHA2-512 (A5525)	KAT	CAST	On demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
HMAC-SHA2-512 (A5526)	KAT	CAST	On demand	Manually
HMAC-SHA2-512 (A5539)	KAT	CAST	On demand	Manually
HMAC-SHA2-512 (A5540)	KAT	CAST	On demand	Manually
HMAC-SHA2-512 (A5541)	KAT	CAST	On demand	Manually
HMAC-SHA2-512 (A5664)	KAT	CAST	On demand	Manually
HMAC-SHA3-224 (A5503)	KAT	CAST	On demand	Manually
HMAC-SHA3-224 (A5526)	KAT	CAST	On demand	Manually
HMAC-SHA3-224 (A5664)	KAT	CAST	On demand	Manually
HMAC-SHA3-256 (A5503)	KAT	CAST	On demand	Manually
HMAC-SHA3-256 (A5526)	KAT	CAST	On demand	Manually
HMAC-SHA3-256 (A5664)	KAT	CAST	On demand	Manually
HMAC-SHA3-384 (A5503)	KAT	CAST	On demand	Manually
HMAC-SHA3-384 (A5526)	KAT	CAST	On demand	Manually
HMAC-SHA3-384 (A5664)	KAT	CAST	On demand	Manually
HMAC-SHA3-512 (A5503)	KAT	CAST	On demand	Manually
HMAC-SHA3-512 (A5526)	KAT	CAST	On demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
HMAC-SHA3-512 (A5664)	KAT	CAST	On demand	Manually
Counter DRBG (A5503)	KAT	CAST	On demand	Manually
Counter DRBG (A5505)	KAT	CAST	On demand	Manually
Counter DRBG (A5506)	KAT	CAST	On demand	Manually
Counter DRBG (A5507)	KAT	CAST	On demand	Manually
Counter DRBG (A5508)	KAT	CAST	On demand	Manually
Counter DRBG (A5509)	KAT	CAST	On demand	Manually
Counter DRBG (A5510)	KAT	CAST	On demand	Manually
Counter DRBG (A5511)	KAT	CAST	On demand	Manually
Counter DRBG (A5512)	KAT	CAST	On demand	Manually
Counter DRBG (A5513)	KAT	CAST	On demand	Manually
Counter DRBG (A5514)	KAT	CAST	On demand	Manually
Counter DRBG (A5515)	KAT	CAST	On demand	Manually
Counter DRBG (A5521)	KAT	CAST	On demand	Manually
Counter DRBG (A5522)	KAT	CAST	On demand	Manually
Counter DRBG (A5523)	KAT	CAST	On demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
Counter DRBG (A5526)	KAT	CAST	On demand	Manually
Counter DRBG (A5528)	KAT	CAST	On demand	Manually
Counter DRBG (A5529)	KAT	CAST	On demand	Manually
Counter DRBG (A5530)	KAT	CAST	On demand	Manually
Counter DRBG (A5531)	KAT	CAST	On demand	Manually
Counter DRBG (A5532)	KAT	CAST	On demand	Manually
Counter DRBG (A5533)	KAT	CAST	On demand	Manually
Counter DRBG (A5534)	KAT	CAST	On demand	Manually
Counter DRBG (A5535)	KAT	CAST	On demand	Manually
Counter DRBG (A5536)	KAT	CAST	On demand	Manually
Counter DRBG (A5537)	KAT	CAST	On demand	Manually
Counter DRBG (A5538)	KAT	CAST	On demand	Manually
Counter DRBG (A5661)	KAT	CAST	On demand	Manually
Counter DRBG (A5662)	KAT	CAST	On demand	Manually
Counter DRBG (A5663)	KAT	CAST	On demand	Manually
Counter DRBG (A5664)	KAT	CAST	On demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
Counter DRBG (A5665)	KAT	CAST	On demand	Manually
Counter DRBG (A5666)	KAT	CAST	On demand	Manually
Hash DRBG (A5503)	KAT	CAST	On demand	Manually
Hash DRBG (A5516)	KAT	CAST	On demand	Manually
Hash DRBG (A5517)	KAT	CAST	On demand	Manually
Hash DRBG (A5518)	KAT	CAST	On demand	Manually
Hash DRBG (A5526)	KAT	CAST	On demand	Manually
Hash DRBG (A5539)	KAT	CAST	On demand	Manually
Hash DRBG (A5540)	KAT	CAST	On demand	Manually
Hash DRBG (A5541)	KAT	CAST	On demand	Manually
Hash DRBG (A5664)	KAT	CAST	On demand	Manually
HMAC DRBG (A5503)	KAT	CAST	On demand	Manually
HMAC DRBG (A5516)	KAT	CAST	On demand	Manually
HMAC DRBG (A5517)	KAT	CAST	On demand	Manually
HMAC DRBG (A5518)	KAT	CAST	On demand	Manually
HMAC DRBG (A5526)	KAT	CAST	On demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
HMAC DRBG (A5539)	KAT	CAST	On demand	Manually
HMAC DRBG (A5540)	KAT	CAST	On demand	Manually
HMAC DRBG (A5541)	KAT	CAST	On demand	Manually
HMAC DRBG (A5664)	KAT	CAST	On demand	Manually
ECDSA SigVer (FIPS186-5) (A5504)	KAT	CAST	On demand	Manually
ECDSA SigVer (FIPS186-5) (A5527)	KAT	CAST	On demand	Manually
RSA SigVer (FIPS186-5) (A5503)	KAT	CAST	On demand	Manually
RSA SigVer (FIPS186-5) (A5526)	KAT	CAST	On demand	Manually
RSA SigVer (FIPS186-5) (A5664)	KAT	CAST	On demand	Manually
KDF SP800-108 (A5503)	KAT	CAST	On demand	Manually
KDF SP800-108 (A5526)	KAT	CAST	On demand	Manually
KAS-ECC-SSC Sp800-56Ar3 (A5503)	KAT	CAST	On demand	Manually
KAS-ECC-SSC Sp800-56Ar3 (A5526)	KAT	CAST	On demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
KAS-FFC-SSC Sp800-56Ar3 (A5503)	KAT	CAST	On demand	Manually
KAS-FFC-SSC Sp800-56Ar3 (A5526)	KAT	CAST	On demand	Manually
ECDSA KeyGen (FIPS186-5) (A5503)	PCT	PCT	On demand	Manually
ECDSA KeyGen (FIPS186-5) (A5526)	PCT	PCT	On demand	Manually
Safe Primes Key Generation (A5503)	PCT	PCT	On demand	Manually
Safe Primes Key Generation (A5526)	PCT	PCT	On demand	Manually
Entropy Source - RCT start-up test	RCT	CAST	On demand	Manually
Entropy Source - APT start-up test	APT	CAST	On demand	Manually
Entropy Source - RCT continuous test	RCT	CAST	N/A	N/A
Entropy Source - APT continuous test	APT	CAST	N/A	N/A

Table 24: 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 Failure of pre-operational tests or CASTs Failure of Entropy source Health Tests Failure of PCT tests	Restart of the module	Kernel Panic

Table 25: Error States

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

10.5 Operator Initiation of Self-Tests

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

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

The module is distributed as a part of the SUSE Enterprise Linux SP6 RPM packages in the form of:

- kernel-default-6.4.0-150600.23.25.1 (for x86, aarch64, and s390x platforms)
- kernel-rt-6.4.0-150600.10.17.1 (for x86 platforms)
- libkcapi-tools-0.13.0-150600.17.3.1 (for x86, aarch64, and s390x platforms)
- dracut-fips-059+suse.521.g8412a1c0-150600.1.3 (for x86, aarch64, and s390x platforms)

The module can achieve FIPS validated configuration by:

1. Install the dracut-fips RPM package:

   ```
   # zipper install dracut-fips
   ```

2. Recreate the initramfs image:

   ```
   # dracut -f
   ```

3. After regenerating the initrd, the Crypto Officer must append the following parameter in the /etc/default/grub configuration file in the GRUB_CMDLINE_LINUX_DEFAULT line:

   ```
   fips=1
   ```

4. After editing the configuration file, please run the following command to change the setting in the boot loader depending on if the system uses UEFI boot or legacy boot:

   ```
   # grub2-mkconfig -o /boot/efi/EFI/sles/grub.cfg
   ```

   ```
   # grub2-mkconfig -o /boot/grub2/grub.cfg
   ```

If /boot or /boot/efi resides on a separate partition, the kernel parameter boot=<partition of /boot or /boot/efi> must be supplied. The partition can be identified with the command "df /boot" or "df /boot/efi" respectively. For example:

```
# df /boot
Filesystem     1K-blocks    Used    Available    Use%    Mounted on
/dev/sda1      233191       30454   190296       14%     /boot
```

The partition of /boot is located on /dev/sda1 in this example. Therefore, the following string needs to be appended in the aforementioned grub file:

```
"boot=/dev/sda1"
```

Reboot to apply these settings.

11.2 Administrator Guidance

After the operating environment is configured as adviced in Section 11.1 to support FIPS operation, the Crypto Officer should check the existence of the file /proc/sys/crypto/fips_enabled, and verify it contains a numeric value “1”. If the file does not exist or does not contain “1”, the operating environment is not configured to support FIPS and the module will not operate as a FIPS validated module properly.

Then, the Crypto Officer must execute the following commands, which must output the following:

 # cat /proc/sys/crypto/fips_version
6.4.0-150600.23.25-default (for version 3.5)
6.4.0-150600.10.17-rt (for version 3.6)

 # rpm -q libkcapi-tools
libkcapi-tools-0.13.0-150600.17.3.1 (for versions 3.5 and 3.6)

 # rpm -q dracut-fips
dracut-fips-059+suse.521.g8412a1c0-150600.1.3 (for versions 3.5 and 3.6)

11.3 Non-Administrator Guidance

There is no non-administrator guidance.

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. Then, if desired, the RPMs mentioned in Section 11.1 can be uninstalled from the SUSE Linux Enterprise SP6 system.

12 Mitigation of Other Attacks

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

Appendix A. Glossary and Abbreviations

AES	Advanced Encryption Standard
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
DH	Diffie-Hellman
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
HMAC	Keyed-Hash Message Authentication Code
IKE	Internet Key Exchange
IPsec	Internet Protocol Security

KAS	Key Agreement Scheme
KAT	Known Answer Test
KBKDF	Key-Based Key Derivation Function
KW	Key Wrap
KWP	Key Wrap with Padding
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
PKCS	Public-Key Cryptography Standards
RSA	Rivest, Shamir, Addleman
SHA	Secure Hash Algorithm
SSC	Shared Secret Computation
SSP	Sensitive Security Parameter
TLS	Transport Layer Security
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://doi.org/10.6028/NIST.FIPS.140-3

FIPS 140-3 IG **Implementation Guidance for FIPS PUB 140-3 and the Cryptographic Module Validation Program**
2 September 2025
https://csrc.nist.gov/Projects/cryptographic-module-validation-program/fips-140-3-ig-announcements

FIPS 180-4 **Secure Hash Standard (SHS)**
March 2012
https://doi.org/10.6028/NIST.FIPS.180-4

FIPS 186-4 **Digital Signature Standard (DSS)**
July 2013
https://doi.org/10.6028/NIST.FIPS.186-4

FIPS 186-5 **Digital Signature Standard (DSS)**
February 2023
https://doi.org/10.6028/NIST.FIPS.186-5

FIPS 198-1 **The Keyed Hash Message Authentication Code (HMAC)**
July 2008
https://doi.org/10.6028/NIST.FIPS.198-1

FIPS 202 **SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions**
August 2015
https://doi.org/10.6028/NIST.FIPS.202

PKCS#1 **Public Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1**
February 2003
https://www.ietf.org/rfc/rfc3447.txt

RFC 4106 **The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)**
June 2005
https://www.rfc-editor.org/rfc/rfc4106.txt

RFC 7296	**Internet Key Exchange Protocol Version 2 (IKEv2)** June 2005 https://www.rfc-editor.org/rfc/rfc7296.txt
SP 800-38A	**Recommendation for Block Cipher Modes of Operation Methods and Techniques** December 2001 https://doi.org/10.6028/NIST.SP.800-38A
SP 800-38B	**Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication** May 2005 https://doi.org/10.6028/NIST.SP.800-38B
SP 800-38C	**Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality** May 2004 https://doi.org/10.6028/NIST.SP.800-38C
SP 800-38D	**Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC** November 2007 https://doi.org/10.6028/NIST.SP.800-38D
SP 800-38E	**Recommendation for Block Cipher Modes of Operation: The XTS AES Mode for Confidentiality on Storage Devices** January 2010 https://doi.org/10.6028/NIST.SP.800-38E
SP 800-38F	**Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping** December 2012 https://doi.org/10.6028/NIST.SP.800-38F
SP 800-56A Rev. 3	**Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography** April 2018 https://doi.org/10.6028/NIST.SP.800-56Ar3
SP 800-90A Rev. 1	**Recommendation for Random Number Generation Using Deterministic Random Bit Generators** June 2015 https://doi.org/10.6028/NIST.SP.800-90Ar1

SP 800-108 Rev. 1 **Recommendation for Key Derivation Using Pseudorandom Functions**
August 2022
https://doi.org/10.6028/NIST.SP.800-108r1-upd1

SP 800-133 Rev. 2 **Recommendation for Cryptographic Key Generation**
June 2020
https://doi.org/10.6028/NIST.SP.800-133r2