Canonical Ltd. Ubuntu 24.04 Kernel Crypto API Cryptographic Module

FIPS 140-3 Non-Proprietary Security Policy

Version 1.1

Last update: 01-20-2026

Prepared by:

atsec information security corporation

4516 Seton Center Pkwy, Suite 250

Austin, TX 78759

www.atsec.com

© 2026 Canonical Ltd./ atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Table of Contents

1 General 6
1.1 Overview 6
1.2 Security Levels 6
1.3 Additional Information 6
2 Cryptographic Module Specification 7
2.1 Description 7
2.2 Tested and Vendor Affirmed Module Version and Identification 8
2.3 Excluded Components 10
2.4 Modes of Operation 10
2.5 Algorithms 10
2.6 Security Function Implementations 13
2.7 Algorithm Specific Information 17
2.7.1 AES GCM IV 17
2.7.2 AES XTS 18
2.7.3 Diffie-Hellman and EC Diffie-Hellman 18
2.7.4 SHA-3 18
2.7.5 RSA 19
2.7.6 SHA-1 19
2.8 RBG and Entropy 19
2.9 Key Generation 20
2.10 Key Establishment 20
2.11 Industry Protocols 20
2.12 ECDSA 20
3 Cryptographic Module Interfaces 21
3.1 Ports and Interfaces 21
4 Roles, Services, and Authentication 22
4.1 Authentication Methods 22
4.2 Roles 22
4.3 Approved Services 22
4.4 Non-Approved Services 29
4.5 External Software/Firmware Loaded 29
5 Software/Firmware Security 30
5.1 Integrity Techniques 30
5.2 Initiate on Demand 30
6 Operational Environment 31

© 2026 Canonical Ltd. / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

6.1 Operational Environment Type and Requirements 31
6.2 Configuration Settings and Restrictions 31
7 Physical Security 32
8 Non-Invasive Security 33
9 Sensitive Security Parameters Management 34
9.1 Storage Areas 34
9.2 SSP Input-Output Methods 34
9.3 SSP Zeroization Methods 34
9.4 SSPs 35
9.5 Transitions 39
10 Self-Tests 40
10.1 Pre-Operational Self-Tests 40
10.2 Conditional Self-Tests 40
10.3 Periodic Self-Test Information 61
10.4 Error States 71
10.5 Operator Initiation of Self-Tests 71
11 Life-Cycle Assurance 72
11.1 Installation, Initialization, and Startup Procedures 72
11.2 Administrator Guidance 72
11.3 Non-Administrator Guidance 73
11.4 End of Life 73
12 Mitigation of Other Attacks 74
Appendix A. Glossary and Abbreviations 75
Appendix B. References 76

© 2026 Canonical Ltd. / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

List of Tables

Table 1: Security Levels 6
Table 2: Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets) 8
Table 3: Tested Operational Environments - Software, Firmware, Hybrid 9
Table 4: Vendor-Affirmed Operational Environments - Software, Firmware, Hybrid 9
Table 5: Modes List and Description 10
Table 6: Approved Algorithms 12
Table 7: Vendor-Affirmed Algorithms 12
Table 8: Non-Approved, Not Allowed Algorithms 13
Table 9: Security Function Implementations 17
Table 10: Entropy Certificates 19
Table 11: Entropy Sources 19
Table 12: Ports and Interfaces 21
Table 13: Roles 22
Table 14: Approved Services 28
Table 15: Non-Approved Services 29
Table 16: Storage Areas 34
Table 17: SSP Input-Output Methods 34
Table 18: SSP Zeroization Methods 35
Table 19: SSP Table 1 38
Table 20: SSP Table 2 39
Table 21: Pre-Operational Self-Tests 40
Table 22: Conditional Self-Tests 61
Table 23: Pre-Operational Periodic Information 61
Table 24: Conditional Periodic Information 71
Table 25: Error States 71

© 2026 Canonical Ltd. / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

List of Figures

Figure 1: Block Diagram 7

© 2026 Canonical Ltd. / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

1 General

1.1 Overview

This document is the non-proprietary FIPS 140-3 Security Policy for version 6.8.0-38-fips of the Canonical Ltd. Ubuntu 24.04 Kernel Crypto API Cryptographic Module. It contains the security rules under which the module must operate and describes how this module meets the requirements as specified in FIPS PUB 140-3 (Federal Information Processing Standards Publication 140-3) for an overall Security Level 1 module.

This Non-Proprietary Security Policy may be reproduced and distributed, but only whole and intact and including this notice.

1.2 Security Levels

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

Table 1: Security Levels

1.3 Additional Information

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.

© 2026 Canonical Ltd. / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

2 Cryptographic Module Specification

2.1 Description

Purpose and Use: The Canonical Ltd. Ubuntu 24.04 Kernel Crypto API Cryptographic Module (hereafter referred to as "the module") provides a C language application program interface (API) for use by other (kernel space and user space) processes that require cryptographic functionality. The module operates on a general-purpose computer as part of the Linux kernel. Its cryptographic functionality can be accessed using the Linux Kernel Crypto API.
Module Type: Software
Module Embodiment: 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 kcapi-hasher binary, which is used to verify the integrity of the software components. In addition, the cryptographic boundary contains the .hmac files which store the expected integrity values for each of the software components.

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

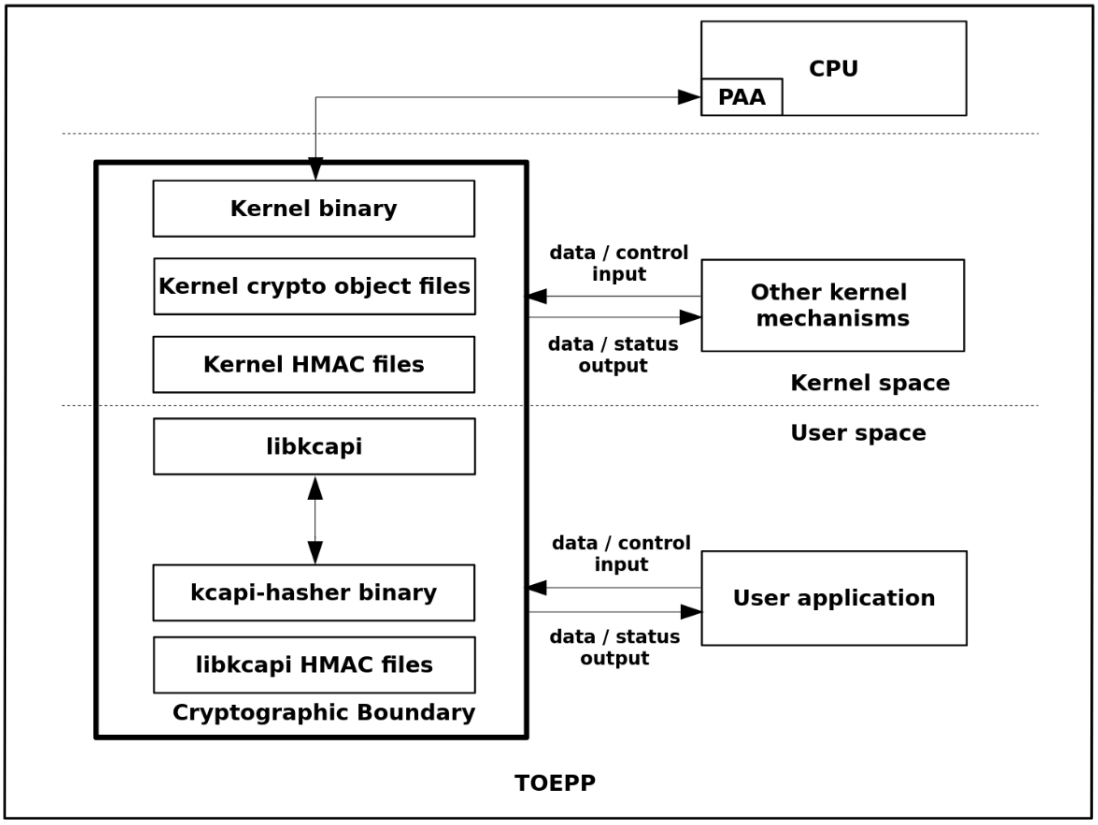

Figure 1: Block Diagram

© 2026 Canonical Ltd. / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Hardware:
N/A for this module.

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

Package or File Name	Software/ Firmware Version	Features	Integrity Test
/boot/vmlinuz-6.8.0-38-fips; *.ko files in /usr/lib/modules/6.8.0-38-fips/kernel/crypto/, *.ko files in /usr/lib/modules/6.8.0-38-fips/kernel/arch/x86/crypto/; /usr/lib/*-linux-gnu/libkcapi.so.1.5.0; /usr/bin/kcapi-hasher	Kernel: 6.8.0-38-fips; libkcapi: 1.4.0-1ubuntu4	N/A	HMAC SHA-512 (vmlinuz-6.8.0-38-fips, libkcapi.so.1.5.0, kcapi-hasher), RSA signature verification (*.ko files)
/boot/vmlinuz-6.8.0-38-fips; *.ko files in /usr/lib/modules/6.8.0-38-fips/kernel/crypto/, *.ko files in /usr/lib/modules/6.8.0-38-fips/kernel/arch/arm64/crypto/; /usr/lib/*-linux-gnu/libkcapi.so.1.5.0; /usr/bin/kcapi-hasher	Kernel: 6.8.0-38-fips; libkcapi: 1.4.0-1ubuntu4	N/A	HMAC SHA-512 (vmlinuz-6.8.0-38-fips, libkcapi.so.1.5.0, kcapi-hasher), RSA signature verification (*.ko files)
/run/mnt/kernel/kernel.efi; *.ko files in /usr/lib/modules/6.8.0-38-fips/kernel/crypto/, *.ko files in /usr/lib/modules/6.8.0-38-fips/kernel/arch/x86/crypto/; /usr/lib/*-linux-gnu/libkcapi.so.1.5.0; /usr/bin/kcapi-hasher	Kernel: 6.8.0-38-fips; libkcapi: 1.4.0-1ubuntu4	N/A	HMAC SHA-512 (kernel.efi, libkcapi.so.1.5.0, kcapi-hasher), RSA signature verification (*.ko files)
/run/mnt/kernel/kernel.efi; *.ko files in /usr/lib/modules/6.8.0-38-fips/kernel/crypto/, *.ko files in /usr/lib/modules/6.8.0-38-fips/kernel/arch/arm64/crypto/; /usr/lib/*-linux-gnu/libkcapi.so.1.5.0; /usr/bin/kcapi-hasher	Kernel: 6.8.0-38-fips; libkcapi: 1.4.0-1ubuntu4	N/A	HMAC SHA-512 (kernel.efi, libkcapi.so.1.5.0, kcapi-hasher), RSA signature verification (*.ko files)

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

Tested Module Identification – Hybrid Disjoint Hardware:
N/A for this module.

Tested Operational Environments - Software, Firmware, Hybrid:

© 2026 Canonical Ltd. / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

The module makes use of hardware acceleration provided by the hardware platform. Namely, AES-NI from the Intel based platform, and NEON and Cryptography Extension (CE) for the Graviton3 based platform, listed in the *Tested Operational Environments - Software, Firmware, Hybrid* table. AES-NI, SHA extensions, NEON, and Cryptography Extensions are considered as PAA.

Operating System	Hardware Platform	Processors	PAA/PAI	Hypervisor or Host OS	Version(s)
Ubuntu 24.04 LTS 64-bit	Supermicro SYS-1019P-WTR	Intel Xeon Gold 6226	Yes	N/A	Kernel: 6.8.0-38-fips Libkcapi: 1.4.0-1ubuntu4
Ubuntu 24.04 LTS 64-bit	Supermicro SYS-1019P-WTR	Intel Xeon Gold 6226	No	N/A	Kernel: 6.8.0-38-fips Libkcapi: 1.4.0-1ubuntu4
Ubuntu Core 24 64-bit	Supermicro SYS-1019P-WTR	Intel Xeon Gold 6226	Yes	N/A	Kernel: 6.8.0-38-fips Libkcapi: 1.4.0-1ubuntu4
Ubuntu Core 24 64-bit	Supermicro SYS-1019P-WTR	Intel Xeon Gold 6226	No	N/A	Kernel: 6.8.0-38-fips Libkcapi: 1.4.0-1ubuntu4
Ubuntu 24.04 LTS 64-bit	Amazon Web Services (AWS) c7g.metal	AWS Graviton3	Yes	N/A	Kernel: 6.8.0-38-fips Libkcapi: 1.4.0-1ubuntu4
Ubuntu 24.04 LTS 64-bit	Amazon Web Services (AWS) c7g.metal	AWS Graviton3	No	N/A	Kernel: 6.8.0-38-fips Libkcapi: 1.4.0-1ubuntu4
Ubuntu Core 24 64-bit	Amazon Web Services (AWS) c7g.metal	AWS Graviton3	Yes	N/A	Kernel: 6.8.0-38-fips Libkcapi: 1.4.0-1ubuntu4
Ubuntu Core 24 64-bit	Amazon Web Services (AWS) c7g.metal	AWS Graviton3	No	N/A	Kernel: 6.8.0-38-fips Libkcapi: 1.4.0-1ubuntu4

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

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

Operating System	Hardware Platform
Ubuntu 24.04 LTS 64-bit	IBM Telum on IBM z16 A01

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.

© 2026 Canonical Ltd. / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

2.3 Excluded Components

Not applicable.

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Type	Status Indicator
Approved mode	Automatically entered whenever an approved service is requested	Approved	Mapped to approved service indicator in Section 4.3 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

Mode Change Instructions and Status:

After passing all pre-operational self-tests and cryptographic algorithm self-tests executed on start-up, the module automatically transitions to the approved mode. No operator intervention is required to reach this point. The module automatically switches between the approved and non-approved modes depending on the services requested by the operator. The status indicator of the mode of operation is equivalent to the indicator of the service that was requested.

2.5 Algorithms

Approved Algorithms:

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	A5588, A5593, A5596, A5599, A5604, A5606, A5609	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CBC-CS3	A5588, A5593, A5596, A5599, A5604, A5606, A5609	Direction - decrypt, encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CCM	A5588, A5593, A5596, A5599, A5609	Key Length - 128, 192, 256	SP 800-38C
AES-CMAC	A5588, A5593, A5596, A5599, A5604, A5609	Direction - Generation, Verification Key Length - 128, 192, 256	SP 800-38B
AES-CTR	A5588, A5593, A5596, A5599, A5604, A5606, A5609	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-ECB	A5588, A5591, A5592, A5593, A5594, A5595, A5596, A5599, A5600, A5601, A5602, A5603, A5604, A5606, A5607, A5608, A5609, A5610, A5611	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-GCM	A5588, A5592, A5593, A5595, A5596, A5599, A5601, A5603, A5606, A5608, A5609, A5611	Direction - Decrypt, Encrypt IV Generation - External Key Length - 128, 192, 256	SP 800-38D

© 2026 Canonical Ltd. / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm	CAVP Cert	Properties	Reference
AES-GCM	A5591, A5594, A5600, A5602, A5607, A5610	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.1 Key Length - 128, 192, 256	SP 800-38D
AES-GMAC	A5588, A5593, A5596, A5599, A5609	Direction - Decrypt, Encrypt IV Generation - External Key Length - 128, 192, 256	SP 800-38D
AES-KW	A5588, A5593, A5599, A5609	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38F
AES-XTS Testing Revision 2.0	A5588, A5593, A5596, A5599, A5604, A5606, A5609	Direction - Decrypt, Encrypt Key Length - 128, 256	SP 800-38E
Counter DRBG	A5588, A5591, A5592, A5593, A5594, A5595, A5599, A5600, A5601, A5602, A5603, A5606, A5607, A5608, A5609, A5610, A5611	Prediction Resistance - No, Yes Mode - AES-128, AES-192, AES-256 Derivation Function Enabled - Yes	SP 800-90A Rev. 1
ECDSA KeyGen (FIPS186-5)	A5588	Curve - P-256, P-384 Secret Generation Mode - testing candidates	FIPS 186-5
ECDSA SigVer (FIPS186-4)	A5589	Component - No Curve - P-256, P-384 Hash Algorithm - SHA-1	FIPS 186-4
ECDSA SigVer (FIPS186-5)	A5589	Curve - P-256, P-384 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA3-256, SHA3-384, SHA3-512	FIPS 186-5
Hash DRBG	A5588, A5612, A5613, A5614	Prediction Resistance - No, Yes Mode - SHA2-256, SHA2-512	SP 800-90A Rev. 1
HMAC DRBG	A5588, A5612, A5613, A5614	Prediction Resistance - No, Yes Mode - SHA2-256, SHA2-512	SP 800-90A Rev. 1
HMAC-SHA-1	A5588, A5596, A5612, A5613, A5614	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-224	A5588, A5596, A5604, A5605, A5612, A5613, A5614	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-256	A5588, A5596, A5604, A5605, A5612, A5613, A5614	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-384	A5588, A5598, A5605, A5612, A5613, A5614	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-512	A5588, A5598, A5605, A5612, A5613, A5614	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA3-224	A5588, A5597	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA3-256	A5588, A5597	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA3-384	A5588, A5597	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA3-512	A5588, A5597	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
KAS-ECC-SSC Sp800-56Ar3	A5588	Domain Parameter Generation Methods - P-256, P-384 Scheme - ephemeralUnified - KAS Role - initiator, responder	SP 800-56A Rev. 3

© 2026 Canonical Ltd. / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm	CAVP Cert	Properties	Reference
KAS-FFC-SSC Sp800-56Ar3	A5588	Domain Parameter Generation Methods - ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192 Scheme - dhEphem - KAS Role - initiator, responder	SP 800-56A Rev. 3
RSA SigVer (FIPS186-4)	A5588	Signature Type - PKCS 1.5 Modulo - 2048, 3072, 4096	FIPS 186-4
RSA SigVer (FIPS186-5)	A5588, A5590	Modulo - 2048, 3072, 4096 Signature Type - pkcs1v1.5	FIPS 186-5
Safe Primes Key Generation	A5588	Safe Prime Groups - ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192	SP 800-56A Rev. 3
SHA-1	A5588, A5596, A5612, A5613, A5614	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2	FIPS 180-4
SHA2-224	A5588, A5596, A5604, A5605, A5612, A5613, A5614	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2	FIPS 180-4
SHA2-256	A5588, A5596, A5604, A5605, A5612, A5613, A5614	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2	FIPS 180-4
SHA2-384	A5588, A5598, A5605, A5612, A5613, A5614	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2	FIPS 180-4
SHA2-512	A5588, A5598, A5605, A5612, A5613, A5614	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2	FIPS 180-4
SHA3-224	A5588, A5597	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2	FIPS 202
SHA3-256	A5588, A5597	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2	FIPS 202
SHA3-384	A5588, A5597	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2	FIPS 202
SHA3-512	A5588, A5597	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2	FIPS 202

Table 6: Approved Algorithms

Vendor-Affirmed Algorithms:

Name	Properties	Implementation	Reference
ECC and DH CKG	Key Type:Asymmetric	N/A	SP800-133r2, 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:

© 2026 Canonical Ltd. / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

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 (libkcapi)	Key derivation with implementation not tested by CAVP
HKDF (libkcapi)	Key derivation with implementation not tested by CAVP
PBKDF2 (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)
KAS-IFC-SSC	Shared secret computation not tested by CAVP

Table 8: Non-Approved, Not Allowed Algorithms

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
Encryption and Decryption with AES	BC-UnAuth	SP800-38A. Encryption, Decryption		AES-CBC: (A5588, A5593, A5596, A5599, A5604, A5606, A5609) AES-ECB: (A5588, A5591, A5592, A5593, A5594, A5595, A5596, A5599, A5600, A5601, A5602, A5603, A5604, A5606, A5607, A5608, A5609, A5610, A5611) AES-CBC-CS3: (A5588, A5593, A5596, A5599, A5604, A5606, A5609) AES-XTS Testing Revision 2.0: (A5588, A5593, A5596, A5599, A5604, A5606, A5609)
Random Number Generation with HMAC DRBG, Hash DRBG or Counter DRBG	DRBG	SP800-90Ar1. Random number generation		Hash DRBG: (A5588, A5612, A5613, A5614) HMAC DRBG: (A5588, A5612, A5613, A5614) Counter DRBG: (A5588, A5591,

© 2026 Canonical Ltd. / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Type	Description	Properties	Algorithms
				A5592, A5593, A5594, A5595, A5599, A5600, A5601, A5602, A5603, A5606, A5607, A5608, A5609, A5610, A5611)
Message Authentication Code Generation with AES or HMAC	MAC	SP800-38B, SP800-38D, FIPS 198-1. Message authentication		HMAC-SHA-1: (A5588, A5596, A5612, A5613, A5614) HMAC-SHA2-224: (A5588, A5596, A5604, A5605, A5612, A5613, A5614) HMAC-SHA2-256: (A5588, A5596, A5604, A5605, A5612, A5613, A5614) HMAC-SHA2-384: (A5588, A5598, A5605, A5612, A5613, A5614) HMAC-SHA2-512: (A5588, A5598, A5605, A5612, A5613, A5614) AES-CMAC: (A5588, A5593, A5596, A5599, A5604, A5609) AES-GMAC: (A5588, A5593, A5596, A5599, A5609) HMAC-SHA3-224: (A5588, A5597) HMAC-SHA3-256: (A5588, A5597) HMAC-SHA3-384: (A5588, A5597) HMAC-SHA3-512: (A5588, A5597)
Message Authentication Code Verification with AES-GMAC	MAC	SP800-38D, FIPS 198-1. Message authentication		AES-GMAC: (A5588, A5593, A5596, A5599, A5609)
Shared Secret Computation with KAS-FFC-SSC or KAS-ECC-SSC	KAS-SSC	SP 800-56Ar3. KAS-ECC-SSC and KAS-FFC-SSC per IG D.F Scenario 2 (1)	KAS-ECC-SSC Sp800-56Ar3 strength:128-192 bits KAS-FFC-SSC Sp800-56Ar3	KAS-ECC-SSC Sp800-56Ar3: (A5588) KAS-FFC-SSC Sp800-56Ar3: (A5588)

© 2026 Canonical Ltd. / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Type	Description	Properties	Algorithms
			strength:112-200 bits	
Message Digest with SHA	SHA	FIPS180-4, FIPS202. Message digest		SHA-1: (A5588, A5596, A5612, A5613, A5614) SHA2-224: (A5588, A5596, A5604, A5605, A5612, A5613, A5614) SHA2-256: (A5588, A5596, A5604, A5605, A5612, A5613, A5614) SHA2-384: (A5588, A5598, A5605, A5612, A5613, A5614) SHA2-512: (A5588, A5598, A5605, A5612, A5613, A5614) SHA3-224: (A5588, A5597) SHA3-256: (A5588, A5597) SHA3-384: (A5588, A5597) SHA3-512: (A5588, A5597)
Key Pair Generation with ECDSA or Safe Primes	AsymKeyPair-KeyGen CKG	FIPS186-5, SP800-56Ar3. ECDSA Key pair generation according to FIPS186-5, Appendix A.2.2 per IG D.H; Safe Primes Key Generation according to SP800-56Ar3, Section 5.6.1.1.4 per IG D.H	KAS-ECC-SSC Sp800-56Ar3 curves:128, 192 bits of strength KAS-FFC-SSC Sp800-56Ar3 key sizes:112-200 bits of strength	Safe Primes Key Generation: (A5588) ECDSA KeyGen (FIPS186-5): (A5588) ECC and DH CKG: ()
Authenticated Encryption and Authenticated Decryption with AES-CCM	BC-Auth	SP800-38C. Authenticated encryption, Authenticated decryption		AES-CCM: (A5588, A5593, A5596, A5599, A5609)
Authenticated Decryption with AES-GCM	BC-AuthDecrypt	SP800-38D. Authenticated decryption		AES-GCM: (A5588, A5591, A5592, A5593, A5594, A5595, A5596, A5599, A5600, A5601, A5602, A5603, A5606, A5607, A5608, A5609, A5610, A5611)

© 2026 Canonical Ltd. / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Type	Description	Properties	Algorithms
Authenticated Encryption and Authenticated Decryption with AES-CBC or AES-CTR with HMAC	BC-Auth	SP800-38A, FIPS 198-1. Authenticated encryption, authenticated decryption.		AES-CBC: (A5588, A5593, A5596, A5599, A5604, A5606, A5609) AES-CTR: (A5588, A5593, A5596, A5599, A5604, A5606, A5609) HMAC-SHA-1: (A5588, A5596, A5612, A5613, A5614) HMAC-SHA2-224: (A5588, A5596, A5604, A5605, A5612, A5613, A5614) HMAC-SHA2-256: (A5588, A5596, A5604, A5605, A5612, A5613, A5614) HMAC-SHA2-384: (A5588, A5598, A5605, A5612, A5613, A5614) HMAC-SHA2-512: (A5588, A5598, A5605, A5612, A5613, A5614)
Signature Verification with RSA	DigSig-SigVer	Signature verification		RSA SigVer (FIPS186-5): (A5588, A5590) SHA2-224: (A5588, A5596, A5604, A5605, A5612, A5613, A5614) SHA2-256: (A5588, A5596, A5604, A5605, A5612, A5613, A5614) SHA2-384: (A5588, A5598, A5605, A5612, A5613, A5614) SHA2-512: (A5588, A5598, A5605, A5612, A5613, A5614)
Signature Verification with ECDSA	DigSig-SigVer	Signature verification		SHA2-224: (A5588, A5596, A5604, A5605, A5612, A5613, A5614) SHA2-256: (A5588, A5596, A5604,

© 2026 Canonical Ltd. / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Type	Description	Properties	Algorithms
				A5605, A5612, A5613, A5614) SHA2-384: (A5588, A5598, A5605, A5612, A5613, A5614) SHA2-512: (A5588, A5598, A5605, A5612, A5613, A5614) ECDSA SigVer (FIPS186-5): (A5589) SHA3-256: (A5588, A5597) SHA3-384: (A5588, A5597) SHA3-512: (A5588, A5597)
Authenticated Encryption and Authenticated Decryption with AES-KW	BC-Auth	SP 800-38F. Authenticated encryption, Authenticated decryption		AES-KW: (A5588, A5593, A5599, A5609)
Legacy Signature Verification with RSA	DigSig-SigVer	Legacy Signature verification	Publications:FIPS 140-3 IG C.M legacy algorithms	SHA-1: (A5588, A5596, A5612, A5613, A5614) RSA SigVer (FIPS186-4): (A5588)
Legacy Signature Verification with ECDSA	DigSig-SigVer	Legacy Signature verification	Publications:FIPS 140-3 IG C.M legacy algorithms	ECDSA SigVer (FIPS186-4): (A5589) SHA-1: (A5588, A5596, A5612, A5613, A5614)

Table 9: Security Function Implementations

2.7 Algorithm Specific Information

2.7.1 AES GCM IV

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

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

© 2026 Canonical Ltd. / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

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

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

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

2.7.2 AES XTS

The length of a single data unit encrypted or decrypted with AES XTS shall not exceed 2^{20} AES blocks, that is 16MB, of data per XTS instance. An XTS instance is defined in Section 4 of SP 800-38E.

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

To meet the requirement stated in IG C.I, the module implements a check to ensure that the two AES keys used in AES XTS mode are not identical. Key_1 and Key_2 shall be generated and/or established independently according to the rules for component symmetric keys from NIST SP 800-133r2, Section 6.3.

2.7.3 Diffie-Hellman and EC Diffie-Hellman

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

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

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

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

2.7.4 SHA-3

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

© 2026 Canonical Ltd. / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

2.7.5 RSA

The module implements FIPS 186-4 RSA SigVer and FIPS 186-5 RSA SigVer. All RSA modulus lengths (i.e., 2048, 3072, 4096 bits) have been CAVP tested. The CAVP certificates are listed in the *Approved Algorithms* table. Algorithms designated as "Legacy" can only be used on data that was generated prior to the Legacy Date specified in FIPS 140-3 IG C.M.

2.7.6 SHA-1

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

2.8 RBG and Entropy

Cert Number	Vendor Name
E243	Canonical Ltd.

Table 10: Entropy Certificates

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
Canonical Ltd. Kernel CPU Time Jitter RNG Entropy Source Version 3.4.0	Non-Physical	Ubuntu 24.04 LTS on Intel Xeon Gold 6226 on Supermicro SYS-1019P-WTR; Ubuntu 24.04 LTS on AWS Graviton3 on Amazon Web Services (AWS) c7g.metal; Ubuntu Core 24 on Intel Xeon Gold 6226 on Supermicro SYS-1019P-WTR; Ubuntu Core 24 on AWS Graviton3 on Amazon Web Services (AWS) c7g.metal	256 bits	256 bits	SHA3-256 (A5588)

Table 11: Entropy Sources

The module implements three different Deterministic Random Bit Generator (DRBG) implementations based on SP 800-90Ar1: Counter DRBG, Hash DRBG, and HMAC DRBG. Each of these DRBG implementations can be instantiated by the operator of the module, using the parameters listed specified in the *Security Function Implementations* table. When instantiated, these DRBGs can be used to generate random numbers for external usage. Additionally, the module employs a specific HMAC-SHA-512 DRBG implementation for internal purposes (e.g. to generate asymmetric key pairs).

The module complies with the Public Use Document for ESV certificate E243 by reading entropy data from the jent_kcapi_random() function, which corresponds to the GetEntropy() conceptual interface. This function outputs 256 bits of full entropy.

The HMAC-SHA-512 DRBG is instantiated with a 384-bit entropy input and reseeded with a 256-bits long entropy input. 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.

© 2026 Canonical Ltd. / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

2.9 Key Generation

The module implements Cryptographic Key Generation (CKG, vendor affirmed), compliant with SP 800-133r2. When random values are required, they are directly obtained as output from the SP 800-90Ar1 approved DRBG, compliant with Section 4 of SP 800-133r2 (without XOR, as described in Additional Comment 2 of IG D.H).

The following methods are implemented: Safe Primes key pair generation and ECDSA key pair generation

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

2.10 Key Establishment

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. These are KAS-FFC-SSC and KAS-ECC-SSC

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. These are AES-KW, AES-CCM, AES-GCM, and AES-CBC or AES-CTR with HMAC SHA-1, HMAC SHA-256, HMAC SHA-384, or HMAC SHA-512.

2.11 Industry Protocols

AES-GCM with internal IV generation in the approved mode is compliant with RFC 4106 and shall only be used in conjunction with the IPsec protocol.

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

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

For Elliptic Curve Diffie-Hellman, the module supports the use of the following curves:

- TLS (RFC 4492): P-256 (secp256r1), P-384 (secp384r1)

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

2.12 ECDSA

The module implements FIPS 186-4 ECDSA SigVer and FIPS 186-5 ECDSA SigVer. Algorithms designated as “Legacy” can only be used on data that was generated prior to the Legacy Date specified in FIPS 140-3 IG C.M.

© 2026 Canonical Ltd. / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

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

Table 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. The module does not implement a control output interface.

© 2026 Canonical Ltd. / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

4 Roles, Services, and Authentication

4.1 Authentication Methods

N/A for this module.

4.2 Roles

Name	Type	Operator Type	Authentication Methods
CO	Role	CO	None

Table 13: Roles

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

4.3 Approved Services

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Message Digest	Compute a message digest	crypto_shash_init returns 0	Message	Digest Value	Message Digest with SHA	CO
Encryption	Encrypt a plaintext	crypto_skcipher_setkey returns 0	AES Key, plaintext	Ciphertext	Encryption and Decryption with AES	CO - AES Key: W,E
Decryption	Decrypt a ciphertext	crypto_skcipher_setkey returns 0	AES Key, ciphertext	Plaintext	Encryption and Decryption with AES	CO - AES Key: W,E
Authenticated Encryption	Encrypt a plaintext	crypto_aead_setkey returns 0	AES Key, IV, plaintext	Ciphertext, MAC tag	Authenticated Encryption and Authenticated Decryption with AES-CCM Authenticated Encryption and Authenticated Decryption with AES-CBC or AES-CTR with HMAC	CO - AES Key: W,E

© 2026 Canonical Ltd. / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					Authenticated Encryption and Authenticated Decryption with AES-KW	
Authenticated Decryption	Decrypt a ciphertext	For all except AES GCM: crypto_aead_setkey returns 0; For AES GCM: crypto_aead_get_flags(tfm) has the CRYPTO_ALG_FIPS140_COMPLIANT flag set	AES key, IV, MAC tag, ciphertext	Plaintext or failure	Authenticated Encryption and Authenticated Decryption with AES-CCM Authenticated Decryption with AES-GCM Authenticated Encryption and Authenticated Decryption with AES-CBC or AES-CTR with HMAC Authenticated Encryption and Authenticated Decryption with AES-KW	CO - AES Key: W,E
Message Authentication Code Generation	Compute a MAC tag	crypto_shash_init returns 0	AES Key or HMAC key, message	MAC tag	Message Authentication Code Generation with AES or HMAC	CO - AES Key: W,E - HMAC Key: W,E
Message Authentication Code Verification	Verify a MAC tag	crypto_shash_init returns 0	AES key, MAC tag, message	Pass/fail	Message Authentication Code Verification	CO - AES Key: W,E

© 2026 Canonical Ltd. / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					with AES-GMAC	
Random Number Generation	Generate random bytes	crypto_rng_get_bytes returns 0	Output length	Random bytes	Random Number Generation with HMAC DRBG, Hash DRBG or Counter DRBG	CO - Entropy Input (IG D.L): W,E,Z - CTR_DRBG Seed (IG D.L): G,E - Hash_DRBG Seed (IG D.L): G,E - HMAC_DRBG Seed (IG D.L): G,E - CTR_DRBG Internal State (V, Key) (IG D.L): G,W,E - Hash_DRBG Internal State (V, C) (IG D.L): G,W,E - HMAC_DRBG Internal State (V, Key) (IG D.L): G,W,E
Shared Secret Computation	Compute a shared secret	crypto_kpp_compute_shared_secret returns 0	DH private key, DH public key or EC private key, EC public key	Shared secret	Shared Secret Computation with KAS-FFC-SSC or KAS-ECC-SSC	CO - DH Public Key: W,E - DH Private Key: W,E - EC Public Key: W,E - EC Private Key: W,E - Shared Secret: G,R
Key Pair Generation	Generate a key pair	crypto_kpp_set_secret and crypto_kpp_generate_public_key return 0	Safe Primes: Group;	Safe Primes: DH	Key Pair Generation with ECDSA	CO - Intermedia

© 2026 Canonical Ltd. / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
			ECDSA: Curve	private key, DH public key; ECDSA: EC private key, EC public key	or Safe Primes	te Key Generation Value: G,E,Z - DH Public Key: G,R - DH Private Key: G,R - EC Public Key: G,R - EC Private Key: G,R
Signature Verification	Verify a signature	crypto_akcipher_init returns 0	Signature, ECDSA public key, RSA public key	Digital signature verification result	Signature Verification with RSA Signature Verification with ECDSA Legacy Signature Verification with RSA Legacy Signature Verification with ECDSA	CO - RSA Public Key: W,E - EC Public Key: W,E
Error Detection Code	Compute an EDC (crc32, crct10dif, crc64-rocksoft)	None	Message	EDC	None	CO
Compression	Compress data (deflate, deflate-iaa, lz4, lz4hc, lzo, zstd)	None	Data	Compressed data	None	CO
Generic System Call	Use the kernel to perform various non-cryptographic operations	None	Identifier, various arguments	Various return values	None	CO
Show Version	Return the module name and version	None	N/A	Module name and version	None	CO

© 2026 Canonical Ltd. / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	information					
Show Status	Return the module status	None	N/A	Module status	None	CO
Self-Test	Perform the CASTs and integrity tests	None	N/A	Pass/fail	Encryption and Decryption with AES Random Number Generation with HMAC DRBG, Hash DRBG or Counter DRBG Message Authentication Code Generation with AES or HMAC Message Authentication Code Verification with AES-GMAC Shared Secret Computation with KAS-FFC-SSC or KAS-ECC-SSC Message Digest with SHA Key Pair Generation with ECDSA or Safe Primes Authenticated Encryption and Authenticated Decryption with AES-CCM Authenticat	CO

© 2026 Canonical Ltd. / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					ed Decryption with AES-GCM Authenticated Encryption and Authenticated Decryption with AES-CBC or AES-CTR with HMAC Signature Verification with RSA Signature Verification with ECDSA Authenticated Encryption and Authenticated Decryption with AES-KW Legacy Signature Verification with RSA Legacy Signature Verification with ECDSA	
Zeroization	Zeroize all SSPs	None	Any SSP	N/A	None	CO - AES Key: Z - HMAC Key: Z - Shared Secret: Z - Entropy Input (IG D.L): Z - CTR_DRBG Seed (IG D.L): Z - Hash_DRB

© 2026 Canonical Ltd. / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						G Seed (IG D.L): Z - HMAC_DRBG Seed (IG D.L): Z - CTR_DRBG Internal State (V, Key) (IG D.L): Z - Hash_DRBG Internal State (V, C) (IG D.L): Z - HMAC_DRBG Internal State (V, Key) (IG D.L): Z - DH Public Key: Z - DH Private Key: Z - EC Public Key: Z - EC Private Key: Z - Intermediate Key Generation Value: Z - RSA Public Key: Z

Table 14: Approved Services

The following convention is used to specify access rights to SSPs:

- **Generate (G):** The module generates or derives the SSP.
- **Read (R):** The SSP is read from the module (e.g. the SSP is output).
- **Write (W):** The SSP is updated, imported, or written to the module.
- **Execute (E):** The module uses the SSP in performing a cryptographic operation.
- **Zeroize (Z):** The module zeroizes the SSP.
- **N/A:** The module does not access any SSP or key during its operation.

© 2026 Canonical Ltd. / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

4.4 Non-Approved Services

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

Table 15: Non-Approved Services

4.5 External Software/Firmware Loaded

Not applicable.

© 2026 Canonical Ltd. / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

5 Software/Firmware Security

5.1 Integrity Techniques

The kcapi-hasher binary utilizes the module's HMAC and SHA-512 implementations and verifies it's integrity test and the libkcapi library integrity followed by the integrity test on the static kernel binary. The HMAC key used for this integrity test is stored in libkcapi. The kernel object (.ko) files are verified using RSA signature verification with PKCS#1 v1.5 padding, SHA-512, and a 4096-bit key stored in the kernel.

5.2 Initiate on Demand

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

© 2026 Canonical Ltd. / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Modifiable

How Requirements are Satisfied: the module executes as part of a general-purpose operating system (Canonical Ubuntu 24.04 and Canonical Ubuntu Core 24), which allows modification, loading, and execution of software that is not part of the validated module.

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

6.2 Configuration Settings and Restrictions

The module shall be installed as specified in Section 11.1.

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

© 2026 Canonical Ltd. / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

7 Physical Security

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

© 2026 Canonical Ltd. / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

8 Non-Invasive Security

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

© 2026 Canonical Ltd. / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

9 Sensitive Security Parameters Management

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
RAM	Temporary storage for SSPs used by the Dynamic 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
API input parameters; AF_ALG type sockets (input)	Operator calling application (TOEPP)	Cryptographic module	Plaintext	Manual	Electronic	
API output parameters; AF_ALG type sockets (output)	Cryptographic module	Operator calling application (TOEPP)	Plaintext	Manual	Electronic	

Table 17: SSP Input-Output Methods

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Free cipher handle	Zeroizes the SSPs contained within the cipher handle	Memory occupied by SSPs is overwritten with zeroes, which renders the SSP values irretrievable	By calling the appropriate zeroization functions: AES key: crypto_free_skcipher and crypto_free_aead; HMAC key: crypto_free_shash and crypto_free_ahash; Internal state: crypto_free_rng; DH public & private key: crypto_free_kpp; EC public & private key: crypto_free_kpp; RSA public & private key: crypto_free_akcipher
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
Remove power from the module	De-allocates the volatile memory used to store SSPs	Volatile memory used by the module is overwritten within nanoseconds	By removing power

© 2026 Canonical Ltd. / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Zeroization Method	Description	Rationale	Operator Initiation
		when power is removed.	

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 Encryption; Decryption; Authenticated encryption; Authenticated decryption; Message authentication;	XTS: 128, 256 bits; ECB, CBC, CTR, CFB128, CBC-CTS-CS3, KW, OFB, CCM, GCM, CMAC, GMAC: 128, 192, 256 bits - XTS: 128, 256 bits; ECB, CBC, CTR, CFB128, CBC-CTS-CS3, KW, OFB, CCM, GCM, CMAC, GMAC: 128, 192, 256 bits	Symmetric key - CSP			Encryption and Decryption with AES Message Authentication Code Generation with AES or HMAC Message Authentication Code Verification with AES-GMAC Authenticated Encryption and Authenticated Decryption with AES-CCM Authenticated Decryption with AES-GCM Authenticated Encryption and Authenticated Decryption with AES-CBC or AES-CTR with HMAC
HMAC Key	HMAC key used for Message authentication code (MAC);	112-524288 bits - 112-256 bits	Symmetric key - CSP			Message Authentication Code Generation with AES or HMAC Authenticated Encryption and Authenticated Decryption with AES-CBC

© 2026 Canonical Ltd. / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
						or AES-CTR with HMAC
Shared Secret	Shared secret established during Shared Secret Computation	KAS-FFC-SSC:ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192; KAS-ECC-SSC: P-256, P-384 bits - KAS-FFC-SSC: 112-200 bits; KAS-ECC-SSC: 128, 192 bits	Shared secret - CSP		Shared Secret Computation with KAS-FFC-SSC or KAS-ECC-SSC	
Entropy Input (IG D.L)	Entropy input used to seed the DRBGs	128-384 bits - 128-256 bits	Entropy input - CSP			Random Number Generation with HMAC DRBG, Hash DRBG or Counter DRBG
CTR_DRBG Seed (IG D.L)	DRBG seed derived from Entropy Input	256, 320, 384 bits - 128, 192, 256 bits	Seed - CSP	Random Number Generation with HMAC DRBG, Hash DRBG or Counter DRBG		Random Number Generation with HMAC DRBG, Hash DRBG or Counter DRBG
Hash_DRBG Seed (IG D.L)	DRBG seed derived from Entropy Input	440, 888 bits - 128, 256 bits	Seed - CSP	Random Number Generation with HMAC DRBG, Hash DRBG or Counter DRBG		Random Number Generation with HMAC DRBG, Hash DRBG or Counter DRBG
HMAC_DRBG Seed (IG D.L)	DRBG seed derived from Entropy Input	440, 888 bits - 128, 256 bits	Seed - CSP	Random Number Generation with HMAC DRBG, Hash DRBG or Counter DRBG		Random Number Generation with HMAC DRBG, Hash DRBG or Counter DRBG
CTR_DRBG Internal State (V, Key) (IG D.L)	Internal state of Counter DRBG instance	256, 320, 384 bits - 128, 192, 256 bits	Internal state - CSP	Random Number Generation with HMAC DRBG, Hash DRBG or Counter DRBG		Random Number Generation with HMAC DRBG, Hash DRBG or Counter DRBG

© 2026 Canonical Ltd. / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
Hash_DRBG Internal State (V, C) (IG D.L)	Internal state of Hash DRBG instance	880, 1776 bits - 128, 256 bits	Internal state - CSP	Random Number Generation with HMAC DRBG, Hash DRBG or Counter DRBG		Random Number Generation with HMAC DRBG, Hash DRBG or Counter DRBG
HMAC_DRBG Internal State (V, Key) (IG D.L)	Internal state of HMAC DRBG instance	320, 512, 1024 bits - 128, 256 bits	Internal state - CSP	Random Number Generation with HMAC DRBG, Hash DRBG or Counter DRBG		Random Number Generation with HMAC DRBG, Hash DRBG or Counter DRBG
DH Public Key	Public key used for KAS-FFC-SSC	ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192 - 112-200 bits	Public key - PSP	Key Pair Generation with ECDSA or Safe Primes		Shared Secret Computation with KAS-FFC-SSC or KAS-ECC-SSC
DH Private Key	DH private key used for KAS-FFC-SSC	ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192 - 112-200 bits	Private key - CSP	Key Pair Generation with ECDSA or Safe Primes		Shared Secret Computation with KAS-FFC-SSC or KAS-ECC-SSC
EC Public Key	Public key used for KAS-ECC-SSC	P-256, P-384 - 128, 192 bits	Public key - PSP	Key Pair Generation with ECDSA or Safe Primes		Shared Secret Computation with KAS-FFC-SSC or KAS-ECC-SSC Signature Verification with ECDSA
EC Private Key	EC private key used for KAS-ECC-SSC	P-521, P-384 - 128, 192 bits	Private key - CSP	Key Pair Generation with ECDSA or Safe Primes		Shared Secret Computation with KAS-FFC-SSC or KAS-ECC-SSC
Intermediate Key Generation Value	Intermediate value generated during Key Pair Generation	2048-8192 bits - 112-200 bits	Intermediate value - CSP	Key Pair Generation with ECDSA or Safe Primes		Key Pair Generation with ECDSA or Safe Primes
RSA Public Key	RSA Public key used for Signature Verification with RSA	2048, 3072, or 4096-bits - 112-150 bits	Public key - PSP			Signature Verification with RSA

© 2026 Canonical Ltd. / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Table 19: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
AES Key	API input parameters; AF_ALG_type sockets (input)	RAM:Plaintext	From service invocation to service completion	Free cipher handle Remove power from the module	
HMAC Key	API input parameters; AF_ALG_type sockets (input)	RAM:Plaintext	From service invocation to service completion	Free cipher handle Remove power from the module	
Shared Secret	API output parameters; AF_ALG type sockets (output)	RAM:Plaintext	From service invocation to service completion	Free cipher handle Remove power from the module	DH Public Key:Derived From DH Private Key:Derived From EC Public Key:Derived From EC Private Key:Derived From
Entropy Input (IG D.L)		RAM:Plaintext	From service invocation to service completion	Automatic Remove power from the module	DRBG Seed (IG D.L):Derives
CTR_DRBG Seed (IG D.L)		RAM:Plaintext	From service invocation to service completion	Automatic Remove power from the module	Entropy Input (IG D.L):Derived From CTR_DRBG Internal State (V, Key) (IG D.L):Derives
Hash_DRBG Seed (IG D.L)		RAM:Plaintext	From service invocation to service completion	Automatic Remove power from the module	Entropy Input (IG D.L):Derived From Hash_DRBG Internal State (V, C) (IG D.L):Derives
HMAC_DRBG Seed (IG D.L)		RAM:Plaintext	From service invocation to service completion	Automatic Remove power from the module	Entropy Input (IG D.L):Derived From HMAC_DRBG Internal State (V, Key) (IG D.L):Derives
CTR_DRBG Internal State (V, Key) (IG D.L)		RAM:Plaintext	From service invocation to service completion	Free cipher handle Remove power from the module	CTR_DRBG Seed (IG D.L):Derived From
Hash_DRBG Internal State (V, C) (IG D.L)		RAM:Plaintext	From service invocation to service completion	Free cipher handle Remove power from the module	Hash_DRBG Seed (IG D.L):Derived From
HMAC_DRBG Internal State (V, Key) (IG D.L)		RAM:Plaintext	From service invocation to service completion	Free cipher handle Remove	HMAC_DRBG Seed (IG D.L):Derived From

© 2026 Canonical Ltd. / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
				power from the module	
DH Public Key	API input parameters; AF_ALG_type sockets (input) API output parameters; AF_ALG type sockets (output)	RAM:Plaintext	From service invocation to service completion	Free cipher handle Remove power from the module	DH Private Key:Paired With Shared Secret:Derives Intermediate Key Generation Value:Generated From
DH Private Key	API input parameters; AF_ALG_type sockets (input) API output parameters; AF_ALG type sockets (output)	RAM:Plaintext	From service invocation to service completion	Free cipher handle Remove power from the module	DH Public Key:Paired With Shared Secret:Derives Intermediate Key Generation Value:Generated From
EC Public Key	API input parameters; AF_ALG_type sockets (input) API output parameters; AF_ALG type sockets (output)	RAM:Plaintext	From service invocation to service completion	Free cipher handle Remove power from the module	EC Private Key:Paired With Shared Secret:Derives Intermediate Key Generation Value:Generated From
EC Private Key	API input parameters; AF_ALG_type sockets (input) API output parameters; AF_ALG type sockets (output)	RAM:Plaintext	From service invocation to service completion	Free cipher handle Remove power from the module	EC Public Key:Paired With Shared Secret:Derives Intermediate Key Generation Value:Generated From
Intermediate Key Generation Value		RAM:Plaintext	From service invocation to service completion	Automatic	DH Public Key:Generates DH Private Key:Generates EC Public Key:Generates EC Private Key:Generates
RSA Public Key	API input parameters; AF_ALG_type sockets (input)	RAM:Plaintext	From service invocation to service completion	Automatic	

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.

© 2026 Canonical Ltd. / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

10 Self-Tests

10.1 Pre-Operational Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
HMAC-SHA2-512 (A5614) - x86 kernel	128-bit key	Message Authentication	SW/FW Integrity	Module becomes operational and services are available for use	Used for kernel binary
HMAC-SHA2-512 (A5614) - x86 libkcapi	128-bit key	Message Authentication	SW/FW Integrity	Module becomes operational and services are available for use	Used for libkcapi binary
HMAC-SHA2-512 (A5614) - x86 kcapi-hasher	128-bit key	Message Authentication	SW/FW Integrity	Module becomes operational and services are available for use	Used for kcapi-hasher binary
HMAC-SHA2-512 (A5598) - ARM kernel	128-bit key	Message Authentication	SW/FW Integrity	Module becomes operational and services are available for use	Used for kernel binary
HMAC-SHA2-512 (A5598) - ARM libkcapi	128-bit key	Message Authentication	SW/FW Integrity	Module becomes operational and services are available for use	Used for libkcapi binary
HMAC-SHA2-512 (A5598) - ARM kcapi-hasher	128-bit key	Message Authentication	SW/FW Integrity	Module becomes operational and services are available for use	Used for kcapi-hasher binary
RSA SigVer (FIPS186-5) (A5588)	4096-bit key with SHA-512	Signature Verification	SW/FW Integrity	Module becomes operational and services are available for use	Used for .ko files

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. While the module is executing the self-tests, services are not available, and data output (via the data output interface) is inhibited until the tests are successfully completed. The module transitions to the operational state only after the pre-operational self-tests are passed successfully.

10.2 Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-ECB (A5588) - Encrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A5591) - Encrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A5592) - Encrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test

© 2026 Canonical Ltd. / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-ECB (A5593) - Encrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A5594) - Encrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A5595) - Encrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A5596) - Encrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A5599) - Encrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A5600) - Encrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A5601) - Encrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A5602) - Encrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A5603) - Encrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A5604) - Encrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A5606) - Encrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A5607) - Encrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A5608) - Encrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test

© 2026 Canonical Ltd. / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-ECB (A5609) - Encrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A5610) - Encrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A5611) - Encrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CBC (A5588) - Encrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CBC (A5593) - Encrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CBC (A5596) - Encrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CBC (A5599) - Encrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CBC (A5604) - Encrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CBC (A5606) - Encrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CBC (A5609) - Encrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CBC-CS3 (A5588) - Encrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CBC-CS3 (A5593) - Encrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CBC-CS3 (A5596) - Encrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test

© 2026 Canonical Ltd. / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-CBC-CS3 (A5599) - Encrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CBC-CS3 (A5604) - Encrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CBC-CS3 (A5606) - Encrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CBC-CS3 (A5609) - Encrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CTR (A5588) - Encrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CTR (A5593) - Encrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CTR (A5596) - Encrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CTR (A5599) - Encrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CTR (A5604) - Encrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CTR (A5606) - Encrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CTR (A5609) - Encrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CCM (A5588) - Encrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CCM (A5593) - Encrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test

© 2026 Canonical Ltd. / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-CCM (A5596) - Encrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CCM (A5599) - Encrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CCM (A5609) - Encrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A5588) - Encrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A5591) - Encrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A5592) - Encrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A5593) - Encrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A5594) - Encrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A5595) - Encrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A5596) - Encrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A5599) - Encrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A5600) - Encrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A5601) - Encrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test

© 2026 Canonical Ltd. / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-GCM (A5602) - Encrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A5603) - Encrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A5606) - Encrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A5607) - Encrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A5608) - Encrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A5609) - Encrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A5610) - Encrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A5611) - Encrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-XTS Testing Revision 2.0 (A5588) - Encrypt	128-bit and 256-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-XTS Testing Revision 2.0 (A5593) - Encrypt	128-bit and 256-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-XTS Testing Revision 2.0 (A5596) - Encrypt	128-bit and 256-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-XTS Testing Revision 2.0 (A5599) - Encrypt	128-bit and 256-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test

© 2026 Canonical Ltd. / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-XTS Testing Revision 2.0 (A5604) - Encrypt	128-bit and 256-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-XTS Testing Revision 2.0 (A5606) - Encrypt	128-bit and 256-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-XTS Testing Revision 2.0 (A5609) - Encrypt	128-bit and 256-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A5588) - Decrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A5591) - Decrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A5592) - Decrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A5593) - Decrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A5594) - Decrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A5595) - Decrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A5596) - Decrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A5599) - Decrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A5600) - Decrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test

© 2026 Canonical Ltd. / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-ECB (A5601) - Decrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A5602) - Decrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A5603) - Decrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A5604) - Decrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A5606) - Decrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A5607) - Decrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A5608) - Decrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A5609) - Decrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A5610) - Decrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A5611) - Decrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CBC (A5588) - Decrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CBC (A5593) - Decrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CBC (A5596) - Decrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test

© 2026 Canonical Ltd. / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-CBC (A5599) - Decrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CBC (A5604) - Decrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CBC (A5606) - Decrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CBC (A5609) - Decrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CBC-CS3 (A5588) - Decrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CBC-CS3 (A5593) - Decrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CBC-CS3 (A5596) - Decrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CBC-CS3 (A5599) - Decrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CBC-CS3 (A5604) - Decrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CBC-CS3 (A5606) - Decrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CBC-CS3 (A5609) - Decrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CTR (A5588) - Decrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CTR (A5593) - Decrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test

© 2026 Canonical Ltd. / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-CTR (A5596) - Decrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CTR (A5599) - Decrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CTR (A5604) - Decrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CTR (A5606) - Decrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CTR (A5609) - Decrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CCM (A5588) - Decrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CCM (A5593) - Decrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CCM (A5596) - Decrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CCM (A5599) - Decrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CCM (A5609) - Decrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A5588) - Decrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A5591) - Decrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A5592) - Decrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test

© 2026 Canonical Ltd. / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-GCM (A5593) - Decrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A5594) - Decrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A5595) - Decrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A5596) - Decrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A5599) - Decrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A5600) - Decrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A5601) - Decrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A5602) - Decrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A5603) - Decrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A5606) - Decrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A5607) - Decrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A5608) - Decrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A5609) - Decrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test

© 2026 Canonical Ltd. / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-GCM (A5610) - Decrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A5611) - Decrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-XTS Testing Revision 2.0 (A5588) - Decrypt	128-bit and 256-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-XTS Testing Revision 2.0 (A5593) - Decrypt	128-bit and 256-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-XTS Testing Revision 2.0 (A5596) - Decrypt	128-bit and 256-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-XTS Testing Revision 2.0 (A5599) - Decrypt	128-bit and 256-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-XTS Testing Revision 2.0 (A5604) - Decrypt	128-bit and 256-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-XTS Testing Revision 2.0 (A5606) - Decrypt	128-bit and 256-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-XTS Testing Revision 2.0 (A5609) - Decrypt	128-bit and 256-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CMAC (A5588)	128-bit and 256-bit key generation	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
AES-CMAC (A5593)	128-bit and 256-bit key generation	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test

© 2026 Canonical Ltd. / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-CMAC (A5596)	128-bit and 256-bit key decrypt	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
AES-CMAC (A5599)	128-bit and 256-bit key generation	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
AES-CMAC (A5604)	128-bit and 256-bit key generation	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
AES-CMAC (A5609)	128-bit and 256-bit key generation	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
SHA-1 (A5588)	SHA-1	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA-1 (A5596)	SHA-1	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA-1 (A5612)	SHA-1	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA-1 (A5613)	SHA-1	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA-1 (A5614)	SHA-1	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-224 (A5588)	SHA2-224	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-224 (A5596)	SHA2-224	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-224 (A5604)	SHA2-224	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-224 (A5605)	SHA2-224	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test

© 2026 Canonical Ltd. / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
SHA2-224 (A5612)	SHA2-224	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-224 (A5613)	SHA2-224	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-224 (A5614)	SHA2-224	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-256 (A5588)	SHA2-256	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-256 (A5596)	SHA2-256	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-256 (A5604)	SHA2-256	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-256 (A5605)	SHA2-256	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-256 (A5612)	SHA2-256	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-256 (A5613)	SHA2-256	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-256 (A5614)	SHA2-256	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-384 (A5588)	SHA2-384	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-384 (A5598)	SHA2-384	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-384 (A5605)	SHA2-384	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test

© 2026 Canonical Ltd. / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
SHA2-384 (A5612)	SHA2-384	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-384 (A5613)	SHA2-384	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-384 (A5614)	SHA2-384	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-512 (A5588)	SHA2-512	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-512 (A5598)	SHA2-512	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-512 (A5605)	SHA2-512	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-512 (A5612)	SHA2-512	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-512 (A5613)	SHA2-512	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-512 (A5614)	SHA2-512	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA3-224 (A5588)	SHA3-224	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA3-224 (A5597)	SHA3-224	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA3-256 (A5588)	SHA3-256	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA3-256 (A5597)	SHA3-256	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test

© 2026 Canonical Ltd. / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
SHA3-384 (A5588)	SHA3-384	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA3-384 (A5597)	SHA3-384	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA3-512 (A5588)	SHA3-512	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA3-512 (A5597)	SHA3-512	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
HMAC-SHA-1 (A5588)	SHA-1	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA-1 (A5596)	SHA-1	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA-1 (A5612)	SHA-1	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA-1 (A5613)	SHA-1	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA-1 (A5614)	SHA-1	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-224 (A5588)	SHA2-224	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-224 (A5596)	SHA2-224	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-224 (A5604)	SHA2-224	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-224 (A5605)	SHA2-224	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test

© 2026 Canonical Ltd. / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HMAC-SHA2-224 (A5612)	SHA2-224	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-224 (A5613)	SHA2-224	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-224 (A5614)	SHA2-224	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-256 (A5588)	SHA2-256	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-256 (A5596)	SHA2-256	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-256 (A5604)	SHA2-256	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-256 (A5605)	SHA2-256	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-256 (A5612)	SHA2-256	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-256 (A5613)	SHA2-256	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-256 (A5614)	SHA2-256	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-384 (A5588)	SHA2-384	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-384 (A5598)	SHA2-384	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-384 (A5605)	SHA2-384	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test

© 2026 Canonical Ltd. / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HMAC-SHA2-384 (A5612)	SHA2-384	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-384 (A5613)	SHA2-384	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-384 (A5614)	SHA2-384	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-512 (A5588)	SHA2-512	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-512 (A5598)	SHA2-512	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-512 (A5605)	SHA2-512	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-512 (A5612)	SHA2-512	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-512 (A5613)	SHA2-512	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-512 (A5614)	SHA2-512	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA3-224 (A5588)	SHA3-224	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA3-224 (A5597)	SHA3-224	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA3-256 (A5588)	SHA3-256	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA3-256 (A5597)	SHA3-256	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test

© 2026 Canonical Ltd. / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HMAC-SHA3-384 (A5588)	SHA3-384	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA3-384 (A5597)	SHA3-384	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA3-512 (A5588)	SHA3-512	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA3-512 (A5597)	SHA3-512	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
Counter DRBG (A5588)	128, 192, 256 bit keys, with/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
Counter DRBG (A5591)	128, 192, 256 bit keys, with/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
Counter DRBG (A5592)	128, 192, 256 bit keys, with/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
Counter DRBG (A5593)	128, 192, 256 bit keys, with/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
Counter DRBG (A5594)	128, 192, 256 bit keys, with/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
Counter DRBG (A5595)	128, 192, 256 bit keys, with/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
Counter DRBG (A5599)	128, 192, 256 bit keys, with/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
Counter DRBG (A5600)	128, 192, 256 bit keys, with/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
Counter DRBG (A5601)	128, 192, 256 bit keys, with/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test

© 2026 Canonical Ltd. / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
Counter DRBG (A5602)	128, 192, 256 bit keys, with/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
Counter DRBG (A5603)	128, 192, 256 bit keys, with/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
Counter DRBG (A5606)	128, 192, 256 bit keys, with/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
Counter DRBG (A5607)	128, 192, 256 bit keys, with/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
Counter DRBG (A5608)	128, 192, 256 bit keys, with/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
Counter DRBG (A5609)	128, 192, 256 bit keys, with/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
Counter DRBG (A5610)	128, 192, 256 bit keys, with/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
Counter DRBG (A5611)	128, 192, 256 bit keys, with/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
Hash DRBG (A5588)	SHA2-256 With/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
Hash DRBG (A5612)	SHA2-256 With/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
Hash DRBG (A5613)	SHA2-256 With/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
Hash DRBG (A5614)	SHA2-256 With/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
HMAC DRBG (A5588)	HMAC-SHA2-256, HMAC-SHA2-512, with/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test

© 2026 Canonical Ltd. / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HMAC DRBG (A5612)	HMAC-SHA2-256, HMAC-SHA2-512, with/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
HMAC DRBG (A5613)	HMAC-SHA2-256, HMAC-SHA2-512, with/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
HMAC DRBG (A5614)	HMAC-SHA2-256, HMAC-SHA2-512, with/without PR	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test	Test runs at power-on before the integrity test
KAS-ECC-SSC Sp800-56Ar3 (A5588)	P-256, P-384 curves	KAT	CAST	Module becomes operational	Shared secret computation	Test runs at power-on before the integrity test
KAS-FFC-SSC Sp800-56Ar3 (A5588)	ffdhe2048	KAT	CAST	Module becomes operational	Shared secret computation	Test runs at power-on before the integrity test
RSA SigVer (FIPS186-4) (A5588)	PKCS#1 v1.5 with 2048 bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
RSA SigVer (FIPS186-5) (A5588)	PKCS#1 v1.5 with 2048 bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
RSA SigVer (FIPS186-5) (A5590)	PKCS#1 v1.5 with 2048 bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
ECDSA SigVer (FIPS186-4) (A5589)	SHA2-256, P-256 curve	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
ECDSA SigVer (FIPS186-5) (A5589)	SHA2-256, P-256 curve	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
Safe Primes Key Generation (A5588)	ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192, Section 5.6.1.1.4 Testing Candidates	PCT	PCT	Successful key pair generation	SP 800-56ARev3, 5.6.2.1.4	Key pair generation
ECDSA KeyGen (FIPS186-5) (A5588)	SHA2-256, P-256, P-384 curves, Appendix A.2.2 Rejection Sampling	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation

© 2026 Canonical Ltd. / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
Entropy Source RCT Startup	1024 samples	RCT	CAST	Module becomes operational and services are available for use	Entropy source startup test	Entropy source initialization
Entropy Source APT Startup	1024 samples	APT	CAST	Module becomes operational and services are available for use	Entropy source startup test	Entropy source initialization
Entropy Source RCT Continuous	Intermittent Cutoff: 31 samples, Permanent Cutoff: 61 samples	RCT	CAST	Entropy source is operational	Entropy source continuous test	Continuously
Entropy Source APT Continuous	512 samples, Intermittent Cutoff: 325 samples, Permanent Cutoff: 355 samples	APT	CAST	Entropy source is operational	Entropy source continuous test	Continuously

Table 22: Conditional Self-Tests

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

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
HMAC-SHA2-512 (A5614) - x86 kernel	Message Authentication	SW/FW Integrity	On Demand	Manually
HMAC-SHA2-512 (A5614) - x86 libkcapi	Message Authentication	SW/FW Integrity	On Demand	Manually
HMAC-SHA2-512 (A5614) - x86 kcapi-hasher	Message Authentication	SW/FW Integrity	On Demand	Manually
HMAC-SHA2-512 (A5598) - ARM kernel	Message Authentication	SW/FW Integrity	On Demand	Manually
HMAC-SHA2-512 (A5598) - ARM libkcapi	Message Authentication	SW/FW Integrity	On Demand	Manually
HMAC-SHA2-512 (A5598) - ARM kcapi-hasher	Message Authentication	SW/FW Integrity	On Demand	Manually
RSA SigVer (FIPS186-5) (A5588)	Signature Verification	SW/FW Integrity	On Demand	Manually

Table 23: Pre-Operational Periodic Information

© 2026 Canonical Ltd. / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-ECB (A5588) - Encrypt	KAT	CAST	On Demand	Manually
AES-ECB (A5591) - Encrypt	KAT	CAST	On Demand	Manually
AES-ECB (A5592) - Encrypt	KAT	CAST	On Demand	Manually
AES-ECB (A5593) - Encrypt	KAT	CAST	On Demand	Manually
AES-ECB (A5594) - Encrypt	KAT	CAST	On Demand	Manually
AES-ECB (A5595) - Encrypt	KAT	CAST	On Demand	Manually
AES-ECB (A5596) - Encrypt	KAT	CAST	On Demand	Manually
AES-ECB (A5599) - Encrypt	KAT	CAST	On Demand	Manually
AES-ECB (A5600) - Encrypt	KAT	CAST	On Demand	Manually
AES-ECB (A5601) - Encrypt	KAT	CAST	On Demand	Manually
AES-ECB (A5602) - Encrypt	KAT	CAST	On Demand	Manually
AES-ECB (A5603) - Encrypt	KAT	CAST	On Demand	Manually
AES-ECB (A5604) - Encrypt	KAT	CAST	On Demand	Manually
AES-ECB (A5606) - Encrypt	KAT	CAST	On Demand	Manually
AES-ECB (A5607) - Encrypt	KAT	CAST	On Demand	Manually
AES-ECB (A5608) - Encrypt	KAT	CAST	On Demand	Manually
AES-ECB (A5609) - Encrypt	KAT	CAST	On Demand	Manually
AES-ECB (A5610) - Encrypt	KAT	CAST	On Demand	Manually
AES-ECB (A5611) - Encrypt	KAT	CAST	On Demand	Manually
AES-CBC (A5588) - Encrypt	KAT	CAST	On Demand	Manually
AES-CBC (A5593) - Encrypt	KAT	CAST	On Demand	Manually
AES-CBC (A5596) - Encrypt	KAT	CAST	On Demand	Manually
AES-CBC (A5599) - Encrypt	KAT	CAST	On Demand	Manually
AES-CBC (A5604) - Encrypt	KAT	CAST	On Demand	Manually
AES-CBC (A5606) - Encrypt	KAT	CAST	On Demand	Manually
AES-CBC (A5609) - Encrypt	KAT	CAST	On Demand	Manually

© 2026 Canonical Ltd. / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-CBC-CS3 (A5588) - Encrypt	KAT	CAST	On Demand	Manually
AES-CBC-CS3 (A5593) - Encrypt	KAT	CAST	On Demand	Manually
AES-CBC-CS3 (A5596) - Encrypt	KAT	CAST	On Demand	Manually
AES-CBC-CS3 (A5599) - Encrypt	KAT	CAST	On Demand	Manually
AES-CBC-CS3 (A5604) - Encrypt	KAT	CAST	On Demand	Manually
AES-CBC-CS3 (A5606) - Encrypt	KAT	CAST	On Demand	Manually
AES-CBC-CS3 (A5609) - Encrypt	KAT	CAST	On Demand	Manually
AES-CTR (A5588) - Encrypt	KAT	CAST	On Demand	Manually
AES-CTR (A5593) - Encrypt	KAT	CAST	On Demand	Manually
AES-CTR (A5596) - Encrypt	KAT	CAST	On Demand	Manually
AES-CTR (A5599) - Encrypt	KAT	CAST	On Demand	Manually
AES-CTR (A5604) - Encrypt	KAT	CAST	On Demand	Manually
AES-CTR (A5606) - Encrypt	KAT	CAST	On Demand	Manually
AES-CTR (A5609) - Encrypt	KAT	CAST	On Demand	Manually
AES-CCM (A5588) - Encrypt	KAT	CAST	On Demand	Manually
AES-CCM (A5593) - Encrypt	KAT	CAST	On Demand	Manually
AES-CCM (A5596) - Encrypt	KAT	CAST	On Demand	Manually
AES-CCM (A5599) - Encrypt	KAT	CAST	On Demand	Manually
AES-CCM (A5609) - Encrypt	KAT	CAST	On Demand	Manually
AES-GCM (A5588) - Encrypt	KAT	CAST	On Demand	Manually
AES-GCM (A5591) - Encrypt	KAT	CAST	On Demand	Manually
AES-GCM (A5592) - Encrypt	KAT	CAST	On Demand	Manually
AES-GCM (A5593) - Encrypt	KAT	CAST	On Demand	Manually
AES-GCM (A5594) - Encrypt	KAT	CAST	On Demand	Manually
AES-GCM (A5595) - Encrypt	KAT	CAST	On Demand	Manually
AES-GCM (A5596) - Encrypt	KAT	CAST	On Demand	Manually
AES-GCM (A5599) - Encrypt	KAT	CAST	On Demand	Manually

© 2026 Canonical Ltd. / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-GCM (A5600) - Encrypt	KAT	CAST	On Demand	Manually
AES-GCM (A5601) - Encrypt	KAT	CAST	On Demand	Manually
AES-GCM (A5602) - Encrypt	KAT	CAST	On Demand	Manually
AES-GCM (A5603) - Encrypt	KAT	CAST	On Demand	Manually
AES-GCM (A5606) - Encrypt	KAT	CAST	On Demand	Manually
AES-GCM (A5607) - Encrypt	KAT	CAST	On Demand	Manually
AES-GCM (A5608) - Encrypt	KAT	CAST	On Demand	Manually
AES-GCM (A5609) - Encrypt	KAT	CAST	On Demand	Manually
AES-GCM (A5610) - Encrypt	KAT	CAST	On Demand	Manually
AES-GCM (A5611) - Encrypt	KAT	CAST	On Demand	Manually
AES-XTS Testing Revision 2.0 (A5588) - Encrypt	KAT	CAST	On Demand	Manually
AES-XTS Testing Revision 2.0 (A5593) - Encrypt	KAT	CAST	On Demand	Manually
AES-XTS Testing Revision 2.0 (A5596) - Encrypt	KAT	CAST	On Demand	Manually
AES-XTS Testing Revision 2.0 (A5599) - Encrypt	KAT	CAST	On Demand	Manually
AES-XTS Testing Revision 2.0 (A5604) - Encrypt	KAT	CAST	On Demand	Manually
AES-XTS Testing Revision 2.0 (A5606) - Encrypt	KAT	CAST	On Demand	Manually
AES-XTS Testing Revision 2.0 (A5609) - Encrypt	KAT	CAST	On Demand	Manually
AES-ECB (A5588) - Decrypt	KAT	CAST	On Demand	Manually
AES-ECB (A5591) - Decrypt	KAT	CAST	On Demand	Manually
AES-ECB (A5592) - Decrypt	KAT	CAST	On Demand	Manually
AES-ECB (A5593) - Decrypt	KAT	CAST	On Demand	Manually
AES-ECB (A5594) - Decrypt	KAT	CAST	On Demand	Manually
AES-ECB (A5595) - Decrypt	KAT	CAST	On Demand	Manually

© 2026 Canonical Ltd. / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-ECB (A5596) - Decrypt	KAT	CAST	On Demand	Manually
AES-ECB (A5599) - Decrypt	KAT	CAST	On Demand	Manually
AES-ECB (A5600) - Decrypt	KAT	CAST	On Demand	Manually
AES-ECB (A5601) - Decrypt	KAT	CAST	On Demand	Manually
AES-ECB (A5602) - Decrypt	KAT	CAST	On Demand	Manually
AES-ECB (A5603) - Decrypt	KAT	CAST	On Demand	Manually
AES-ECB (A5604) - Decrypt	KAT	CAST	On Demand	Manually
AES-ECB (A5606) - Decrypt	KAT	CAST	On Demand	Manually
AES-ECB (A5607) - Decrypt	KAT	CAST	On Demand	Manually
AES-ECB (A5608) - Decrypt	KAT	CAST	On Demand	Manually
AES-ECB (A5609) - Decrypt	KAT	CAST	On Demand	Manually
AES-ECB (A5610) - Decrypt	KAT	CAST	On Demand	Manually
AES-ECB (A5611) - Decrypt	KAT	CAST	On Demand	Manually
AES-CBC (A5588) - Decrypt	KAT	CAST	On Demand	Manually
AES-CBC (A5593) - Decrypt	KAT	CAST	On Demand	Manually
AES-CBC (A5596) - Decrypt	KAT	CAST	On Demand	Manually
AES-CBC (A5599) - Decrypt	KAT	CAST	On Demand	Manually
AES-CBC (A5604) - Decrypt	KAT	CAST	On Demand	Manually
AES-CBC (A5606) - Decrypt	KAT	CAST	On Demand	Manually
AES-CBC (A5609) - Decrypt	KAT	CAST	On Demand	Manually
AES-CBC-CS3 (A5588) - Decrypt	KAT	CAST	On Demand	Manually
AES-CBC-CS3 (A5593) - Decrypt	KAT	CAST	On Demand	Manually
AES-CBC-CS3 (A5596) - Decrypt	KAT	CAST	On Demand	Manually
AES-CBC-CS3 (A5599) - Decrypt	KAT	CAST	On Demand	Manually
AES-CBC-CS3 (A5604) - Decrypt	KAT	CAST	On Demand	Manually
AES-CBC-CS3 (A5606) - Decrypt	KAT	CAST	On Demand	Manually
AES-CBC-CS3 (A5609) - Decrypt	KAT	CAST	On Demand	Manually

© 2026 Canonical Ltd. / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-CTR (A5588) - Decrypt	KAT	CAST	On Demand	Manually
AES-CTR (A5593) - Decrypt	KAT	CAST	On Demand	Manually
AES-CTR (A5596) - Decrypt	KAT	CAST	On Demand	Manually
AES-CTR (A5599) - Decrypt	KAT	CAST	On Demand	Manually
AES-CTR (A5604) - Decrypt	KAT	CAST	On Demand	Manually
AES-CTR (A5606) - Decrypt	KAT	CAST	On Demand	Manually
AES-CTR (A5609) - Decrypt	KAT	CAST	On Demand	Manually
AES-CCM (A5588) - Decrypt	KAT	CAST	On Demand	Manually
AES-CCM (A5593) - Decrypt	KAT	CAST	On Demand	Manually
AES-CCM (A5596) - Decrypt	KAT	CAST	On Demand	Manually
AES-CCM (A5599) - Decrypt	KAT	CAST	On Demand	Manually
AES-CCM (A5609) - Decrypt	KAT	CAST	On Demand	Manually
AES-GCM (A5588) - Decrypt	KAT	CAST	On Demand	Manually
AES-GCM (A5591) - Decrypt	KAT	CAST	On Demand	Manually
AES-GCM (A5592) - Decrypt	KAT	CAST	On Demand	Manually
AES-GCM (A5593) - Decrypt	KAT	CAST	On Demand	Manually
AES-GCM (A5594) - Decrypt	KAT	CAST	On Demand	Manually
AES-GCM (A5595) - Decrypt	KAT	CAST	On Demand	Manually
AES-GCM (A5596) - Decrypt	KAT	CAST	On Demand	Manually
AES-GCM (A5599) - Decrypt	KAT	CAST	On Demand	Manually
AES-GCM (A5600) - Decrypt	KAT	CAST	On Demand	Manually
AES-GCM (A5601) - Decrypt	KAT	CAST	On Demand	Manually
AES-GCM (A5602) - Decrypt	KAT	CAST	On Demand	Manually
AES-GCM (A5603) - Decrypt	KAT	CAST	On Demand	Manually
AES-GCM (A5606) - Decrypt	KAT	CAST	On Demand	Manually
AES-GCM (A5607) - Decrypt	KAT	CAST	On Demand	Manually
AES-GCM (A5608) - Decrypt	KAT	CAST	On Demand	Manually

© 2026 Canonical Ltd. / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-GCM (A5609) - Decrypt	KAT	CAST	On Demand	Manually
AES-GCM (A5610) - Decrypt	KAT	CAST	On Demand	Manually
AES-GCM (A5611) - Decrypt	KAT	CAST	On Demand	Manually
AES-XTS Testing Revision 2.0 (A5588) - Decrypt	KAT	CAST	On Demand	Manually
AES-XTS Testing Revision 2.0 (A5593) - Decrypt	KAT	CAST	On Demand	Manually
AES-XTS Testing Revision 2.0 (A5596) - Decrypt	KAT	CAST	On Demand	Manually
AES-XTS Testing Revision 2.0 (A5599) - Decrypt	KAT	CAST	On Demand	Manually
AES-XTS Testing Revision 2.0 (A5604) - Decrypt	KAT	CAST	On Demand	Manually
AES-XTS Testing Revision 2.0 (A5606) - Decrypt	KAT	CAST	On Demand	Manually
AES-XTS Testing Revision 2.0 (A5609) - Decrypt	KAT	CAST	On Demand	Manually
AES-CMAC (A5588)	KAT	CAST	On Demand	Manually
AES-CMAC (A5593)	KAT	CAST	On Demand	Manually
AES-CMAC (A5596)	KAT	CAST	On Demand	Manually
AES-CMAC (A5599)	KAT	CAST	On Demand	Manually
AES-CMAC (A5604)	KAT	CAST	On Demand	Manually
AES-CMAC (A5609)	KAT	CAST	On Demand	Manually
SHA-1 (A5588)	KAT	CAST	On Demand	Manually
SHA-1 (A5596)	KAT	CAST	On Demand	Manually
SHA-1 (A5612)	KAT	CAST	On Demand	Manually
SHA-1 (A5613)	KAT	CAST	On Demand	Manually
SHA-1 (A5614)	KAT	CAST	On Demand	Manually
SHA2-224 (A5588)	KAT	CAST	On Demand	Manually
SHA2-224 (A5596)	KAT	CAST	On Demand	Manually
SHA2-224 (A5604)	KAT	CAST	On Demand	Manually
SHA2-224 (A5605)	KAT	CAST	On Demand	Manually
SHA2-224 (A5612)	KAT	CAST	On Demand	Manually
SHA2-224 (A5613)	KAT	CAST	On Demand	Manually
SHA2-224 (A5614)	KAT	CAST	On Demand	Manually
SHA2-256 (A5588)	KAT	CAST	On Demand	Manually
SHA2-256 (A5596)	KAT	CAST	On Demand	Manually
SHA2-256 (A5604)	KAT	CAST	On Demand	Manually
SHA2-256 (A5605)	KAT	CAST	On Demand	Manually
SHA2-256 (A5612)	KAT	CAST	On Demand	Manually
SHA2-256 (A5613)	KAT	CAST	On Demand	Manually
SHA2-256 (A5614)	KAT	CAST	On Demand	Manually
SHA2-384 (A5588)	KAT	CAST	On Demand	Manually

© 2026 Canonical Ltd. / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
SHA2-384 (A5598)	KAT	CAST	On Demand	Manually
SHA2-384 (A5605)	KAT	CAST	On Demand	Manually
SHA2-384 (A5612)	KAT	CAST	On Demand	Manually
SHA2-384 (A5613)	KAT	CAST	On Demand	Manually
SHA2-384 (A5614)	KAT	CAST	On Demand	Manually
SHA2-512 (A5588)	KAT	CAST	On Demand	Manually
SHA2-512 (A5598)	KAT	CAST	On Demand	Manually
SHA2-512 (A5605)	KAT	CAST	On Demand	Manually
SHA2-512 (A5612)	KAT	CAST	On Demand	Manually
SHA2-512 (A5613)	KAT	CAST	On Demand	Manually
SHA2-512 (A5614)	KAT	CAST	On Demand	Manually
SHA3-224 (A5588)	KAT	CAST	On Demand	Manually
SHA3-224 (A5597)	KAT	CAST	On Demand	Manually
SHA3-256 (A5588)	KAT	CAST	On Demand	Manually
SHA3-256 (A5597)	KAT	CAST	On Demand	Manually
SHA3-384 (A5588)	KAT	CAST	On Demand	Manually
SHA3-384 (A5597)	KAT	CAST	On Demand	Manually
SHA3-512 (A5588)	KAT	CAST	On Demand	Manually
SHA3-512 (A5597)	KAT	CAST	On Demand	Manually
HMAC-SHA-1 (A5588)	KAT	CAST	On Demand	Manually
HMAC-SHA-1 (A5596)	KAT	CAST	On Demand	Manually
HMAC-SHA-1 (A5612)	KAT	CAST	On Demand	Manually
HMAC-SHA-1 (A5613)	KAT	CAST	On Demand	Manually
HMAC-SHA-1 (A5614)	KAT	CAST	On Demand	Manually
HMAC-SHA2-224 (A5588)	KAT	CAST	On Demand	Manually
HMAC-SHA2-224 (A5596)	KAT	CAST	On Demand	Manually
HMAC-SHA2-224 (A5604)	KAT	CAST	On Demand	Manually
HMAC-SHA2-224 (A5605)	KAT	CAST	On Demand	Manually
HMAC-SHA2-224 (A5612)	KAT	CAST	On Demand	Manually
HMAC-SHA2-224 (A5613)	KAT	CAST	On Demand	Manually
HMAC-SHA2-224 (A5614)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A5588)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A5596)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A5604)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A5605)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A5612)	KAT	CAST	On Demand	Manually

© 2026 Canonical Ltd. / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
HMAC-SHA2-256 (A5613)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A5614)	KAT	CAST	On Demand	Manually
HMAC-SHA2-384 (A5588)	KAT	CAST	On Demand	Manually
HMAC-SHA2-384 (A5598)	KAT	CAST	On Demand	Manually
HMAC-SHA2-384 (A5605)	KAT	CAST	On Demand	Manually
HMAC-SHA2-384 (A5612)	KAT	CAST	On Demand	Manually
HMAC-SHA2-384 (A5613)	KAT	CAST	On Demand	Manually
HMAC-SHA2-384 (A5614)	KAT	CAST	On Demand	Manually
HMAC-SHA2-512 (A5588)	KAT	CAST	On Demand	Manually
HMAC-SHA2-512 (A5598)	KAT	CAST	On Demand	Manually
HMAC-SHA2-512 (A5605)	KAT	CAST	On Demand	Manually
HMAC-SHA2-512 (A5612)	KAT	CAST	On Demand	Manually
HMAC-SHA2-512 (A5613)	KAT	CAST	On Demand	Manually
HMAC-SHA2-512 (A5614)	KAT	CAST	On Demand	Manually
HMAC-SHA3-224 (A5588)	KAT	CAST	On Demand	Manually
HMAC-SHA3-224 (A5597)	KAT	CAST	On Demand	Manually
HMAC-SHA3-256 (A5588)	KAT	CAST	On Demand	Manually
HMAC-SHA3-256 (A5597)	KAT	CAST	On Demand	Manually
HMAC-SHA3-384 (A5588)	KAT	CAST	On Demand	Manually
HMAC-SHA3-384 (A5597)	KAT	CAST	On Demand	Manually
HMAC-SHA3-512 (A5588)	KAT	CAST	On Demand	Manually
HMAC-SHA3-512 (A5597)	KAT	CAST	On Demand	Manually
Counter DRBG (A5588)	KAT	CAST	On Demand	Manually
Counter DRBG (A5591)	KAT	CAST	On Demand	Manually
Counter DRBG (A5592)	KAT	CAST	On Demand	Manually
Counter DRBG (A5593)	KAT	CAST	On Demand	Manually
Counter DRBG (A5594)	KAT	CAST	On Demand	Manually

© 2026 Canonical Ltd. / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
Counter DRBG (A5595)	KAT	CAST	On Demand	Manually
Counter DRBG (A5599)	KAT	CAST	On Demand	Manually
Counter DRBG (A5600)	KAT	CAST	On Demand	Manually
Counter DRBG (A5601)	KAT	CAST	On Demand	Manually
Counter DRBG (A5602)	KAT	CAST	On Demand	Manually
Counter DRBG (A5603)	KAT	CAST	On Demand	Manually
Counter DRBG (A5606)	KAT	CAST	On Demand	Manually
Counter DRBG (A5607)	KAT	CAST	On Demand	Manually
Counter DRBG (A5608)	KAT	CAST	On Demand	Manually
Counter DRBG (A5609)	KAT	CAST	On Demand	Manually
Counter DRBG (A5610)	KAT	CAST	On Demand	Manually
Counter DRBG (A5611)	KAT	CAST	On Demand	Manually
Hash DRBG (A5588)	KAT	CAST	On Demand	Manually
Hash DRBG (A5612)	KAT	CAST	On Demand	Manually
Hash DRBG (A5613)	KAT	CAST	On Demand	Manually
Hash DRBG (A5614)	KAT	CAST	On Demand	Manually
HMAC DRBG (A5588)	KAT	CAST	On Demand	Manually
HMAC DRBG (A5612)	KAT	CAST	On Demand	Manually
HMAC DRBG (A5613)	KAT	CAST	On Demand	Manually
HMAC DRBG (A5614)	KAT	CAST	On Demand	Manually
KAS-ECC-SSC Sp800-56Ar3 (A5588)	KAT	CAST	On Demand	Manually
KAS-FFC-SSC Sp800-56Ar3 (A5588)	KAT	CAST	On Demand	Manually
RSA SigVer (FIPS186-4) (A5588)	KAT	CAST	On Demand	Manually
RSA SigVer (FIPS186-5) (A5588)	KAT	CAST	On Demand	Manually
RSA SigVer (FIPS186-5) (A5590)	KAT	CAST	On Demand	Manually
ECDSA SigVer (FIPS186-4) (A5589)	KAT	CAST	On Demand	Manually
ECDSA SigVer (FIPS186-5) (A5589)	KAT	CAST	On Demand	Manually
Safe Primes Key Generation (A5588)	PCT	PCT	On Demand	Manually

© 2026 Canonical Ltd. / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
ECDSA KeyGen (FIPS186-5) (A5588)	PCT	PCT	On Demand	Manually
Entropy Source RCT Startup	RCT	CAST	On Demand	Manually
Entropy Source APT Startup	APT	CAST	On Demand	Manually
Entropy Source RCT Continuous	RCT	CAST	On Demand	Manually
Entropy Source APT Continuous	APT	CAST	On Demand	Manually

Table 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	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

The software integrity tests, cryptographic algorithm self-tests, and entropy source start-up tests can be invoked on demand by unloading and subsequently re-initializing the module. The pair-wise consistency tests can be invoked on demand by requesting the key pair generation service.

© 2026 Canonical Ltd. / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

On the Ubuntu 24.04 LTS operational environments, the module is distributed in the form of the following deb packages:

- linux-image-6.8.0-38-fips=6.8.0-38.38+fips4
- linux-image-hmac-6.8.0-38-fips=6.8.0-38.38+fips4
- linux-modules-6.8.0-38-fips=6.8.0-38.38+fips4
- libkcapi1=1.4.0-1ubuntu4
- kcapi-tools=1.4.0-1ubuntu4

On the Ubuntu Core 24 operational environments, the module is distributed in the form of the "fips-kernel" snap, with snap-id ZjfoRia9mZzIe2xoWtGxHNUQsSSqjzUK. Revision 28 and 29 are respectively validated for amd64 and arm64 platforms.

Once configuration to access the PPA is complete, the Crypto Officer must use an Ubuntu One account to obtain a token to attach to the machine. This can be done by running the following command and following the instructions:

$ sudo pro attach

The Crypto Officer can then install the Ubuntu packages containing the module using the Advanced Package Tool (APT) with the following commands:

$ sudo pro enable fips-updates

$ sudo reboot

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

Installation of the module on the Ubuntu Core 24 operational environment simply consists of flashing the operating system image to a hard drive, then following the instructions on the screen.

11.2 Administrator Guidance

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

After the image is installed properly as defined in section 11.1, the Crypto Officer must execute the following commands to verify that the module and its associated packages are installed properly:

$ cat /proc/sys/crypto/fips_name

© 2026 Canonical Ltd. / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

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

Ubuntu 24.04 Kernel Crypto API Cryptographic Module

Then, the Crypto Officer must execute:

$ cat /proc/sys/crypto/fips_version

This command must output the following:

6.8.0-38-fips

Then, the Crypto Officer must execute:

$ kcapi-hasher -v

This command must output the following:

kcapi-hasher: libkcapi 1.5.0

On the Ubuntu 24.04 LTS operational environments, versions of the installed packages can be verified using the following command:

$ dpkg-query -W linux-image-6.8.0-38-fips linux-image-hmac-6.8.0-38-fips linux-modules-6.8.0-38-fips libkcapi1 kcapi-tools

On the Ubuntu Core 24 operational environments, revisions of the installed snaps can be verified using the following command:

$ snap list fips-kernel

11.3 Non-Administrator Guidance

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

11.4 End of Life

As the module does not persistently store SSPs, secure sanitization of the module consists of unloading the module. This will zeroize all SSPs in volatile memory.

If desired, the linux-image-6.8.0-38-fips, linux-image-hmac-6.8.0-38-fips, linux-modules-6.8.0-38-fips, linux-modules-extra-6.8.0-38-fips, libkcapi1, fips-initramfs, and kcapi-tools deb packages can be uninstalled from the Ubuntu 24.04 LTS system.

The Ubuntu Core 24 system is distributed as an operating system image, so removing this image will also uninstall the module. Alternatively, the “snap remodel” command can be used to switch to a generic model with a different kernel.

© 2026 Canonical Ltd. / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

12 Mitigation of Other Attacks

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

© 2026 Canonical Ltd. / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Appendix A. Glossary and Abbreviations

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

© 2026 Canonical Ltd. / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Appendix B. References

FIPS 140-3	**FIPS PUB 140-3 - Security Requirements For Cryptographic Modules** March 2019 https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-3.pdf
FIPS 140-3 IG	**Implementation Guidance for FIPS PUB 140-3 and the Cryptographic Module Validation Program (04-18-2025)** https://csrc.nist.gov/Projects/cryptographic-module-validation-program/fips-140-3-ig-announcements
FIPS 180-4	**Secure Hash Standard (SHS)** March 2012 https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf
FIPS 186-4	**Digital Signature Standard (DSS)** July 2013 https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf
FIPS 186-5	**Digital Signature Standard (DSS)** February 2023 https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-5.pdf
FIPS 197	**Advanced Encryption Standard** May 9, 2023 https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197-upd1.pdf
FIPS 198-1	**The Keyed Hash Message Authentication Code (HMAC)** July 2008 https://csrc.nist.gov/publications/fips/fips198-1/FIPS-198-1_final.pdf
FIPS 202	**SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions** August 2015 https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf
PKCS# 1	**Public Key Cryptography Standards (PKCS) # 1: RSA Cryptography Specifications Version 2.1** February 2003 https://www.ietf.org/rfc/rfc3447.txt
RFC 3526	**More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)** May 2003 https://www.ietf.org/rfc/rfc3526.txt
RFC 4106	**The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)** June 2005 https://datatracker.ietf.org/doc/html/rfc4106
RFC 7296	**Internet Key Exchange Protocol Version 2 (IKEv2)** October 2014 https://datatracker.ietf.org/doc/html/rfc7296

© 2026 Canonical Ltd. / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

SP 800-38A	**Recommendation for Block Cipher Modes of Operation Methods and Techniques** December 2001 https://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf
SP 800-38A Addendum	**Recommendation for Block Cipher Modes of Operation: Three Variants of Ciphertext Stealing for CBC Mode** October 2010 https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38a-add.pdf
SP 800-38B	**Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication** May 2005 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-38B.pdf
SP 800-38C	**Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality** May 2004 https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38c.pdf
SP 800-38D	**Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC** November 2007 https://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf
SP 800-38E	**Recommendation for Block Cipher Modes of Operation: The XTS AES Mode for Confidentiality on Storage Devices** January 2010 https://csrc.nist.gov/publications/nistpubs/800-38E/nist-sp-800-38E.pdf
SP 800-38F	**Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping** December 2012 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-38F.pdf
SP 800-56Ar3	**Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography** April 2018 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Ar3.pdf
SP 800-90Ar1	**Recommendation for Random Number Generation Using Deterministic Random Bit Generators** June 2015 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90Ar1.pdf

© 2026 Canonical Ltd. / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

SP 800-90B	**Recommendation for the Entropy Sources Used for Random Bit Generation** January 2018 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90B.pdf
SP 800-133r2	**Recommendation for Cryptographic Key Generation** June 2020 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-133r2.pdf
SP 800-140Br1	**CMVP Security Policy Requirements** March 2020 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-140Br1.pdf

© 2026 Canonical Ltd. / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.