CANONICAL

ubuntu[©]Canonical Ltd.

Canonical Ltd. Ubuntu 22.04 Kernel Crypto API Cryptographic Module

Version 5.15.0-73-fips

FIPS 140-3 Non-Proprietary Security Policy

Version 1.2

Last update: 11-08-2024

Prepared by:

atsec information security corporation

4516 Seton Center Pkwy, Suite 250

Austin, TX 78759

www.atsec.com

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	9
2.4 Modes of Operation	9
2.5 Algorithms	10
2.6 Security Function Implementations	16
2.7 Algorithm Specific Information	26
2.7.1 AES GCM IV	26
2.7.2 AES XTS	26
2.7.3 Diffie-Hellman and EC Diffie-Hellman	26
2.7.4 SHA-3	27
2.7.5 RSA	27
2.8 RBG and Entropy	27
2.9 Key Generation	28
2.10 Key Establishment	28
2.11 Industry Protocols	29
3 Cryptographic Module Interfaces	30
3.1 Ports and Interfaces	
4 Roles, Services, and Authentication	31
4.1 Authentication Methods	31
4.2 Roles	31
4.3 Approved Services	31
4.4 Non-Approved Services	36
4.5 External Software/Firmware Loaded	36
5 Software/Firmware Security	37
5.1 Integrity Techniques	37
5.2 Initiate on Demand	37
6 Operational Environment	38
6.1 Operational Environment Type and Requirements	
6.2 Configuration Settings and Restrictions	
7 Physical Security	39
8 Non-Invasive Security	40

ubuntu[©]Canonical Ltd. Ubuntu 22.04 Kernel Crypto API Cryptographic Module FIPS 140-3 Non-Proprietary Security Policy

9 Sensitive Security Parameters Management	41
9.1 Storage Areas	41
9.2 SSP Input-Output Methods	41
9.3 SSP Zeroization Methods	41
9.4 SSPs	42
9.5 Transitions	45
10 Self-Tests	46
10.1 Pre-Operational Self-Tests	46
10.2 Conditional Self-Tests	48
10.3 Periodic Self-Test Information	84
10.4 Error States	96
10.5 Operator Initiation of Self-Tests	96
11 Life-Cycle Assurance	97
11.1 Installation, Initialization, and Startup Procedures	97
11.2 Administrator Guidance	
11.3 Non-Administrator Guidance	
11.4 End of Life	
12 Mitigation of Other Attacks	
Appendix A. Glossary and Abbreviations	
Appendix B. References	

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: Modes List and Description	9
Table 5: Approved Algorithms	15
Table 6: Vendor-Affirmed Algorithms	15
Table 7: Non-Approved, Not Allowed Algorithms	16
Table 8: Security Function Implementations	26
Table 9: Entropy Certificates	27
Table 10: Entropy Sources	27
Table 11: Ports and Interfaces	30
Table 12: Roles	31
Table 13: Approved Services	35
Table 14: Non-Approved Services	36
Table 15: Storage Areas	41
Table 16: SSP Input-Output Methods	41
Table 17: SSP Zeroization Methods	41
Table 18: SSP Table 1	44
Table 19: SSP Table 2	45
Table 20: Pre-Operational Self-Tests	47
Table 21: Conditional Self-Tests	84
Table 22: Pre-Operational Periodic Information	85
Table 23: Conditional Periodic Information	96
Table 24: Error States	96

ubuntu[©]Canonical Ltd. Ubuntu 22.04 Kernel Crypto API Cryptographic Module FIPS 140-3 Non-Proprietary Security Policy

List of Figures

Figure	: Block Diagram	1
--------	-----------------	---

1 General

1.1 Overview

This document is the non-proprietary FIPS 140-3 Security Policy for version 5.15.0-73-fips of the Canonical Ltd. Ubuntu 22.04 Kernel Crypto API Cryptographic Module. It contains the security rules under which the module must operate and describes how this module meets the requirements as specified in FIPS PUB 140-3 (Federal Information Processing Standards Publication 140-3) for an overall Security Level 1 module.

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

1.2 Security Levels

Section	Security Level
1	1
2	1
3	1
4	1
5	1
6	1
7	N/A
8	N/A
9	1
10	1
11	1
12	N/A
Overall	1

Table 1: Security Levels

1.3 Additional Information

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

2 Cryptographic Module Specification

2.1 Description

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

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

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



Figure 1: Block Diagram

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Hardware:

N/A for this module.

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

Package or File Name	Software/ Firmware Version	Features	Integrity Test
/boot/vmlinuz-5.15.0-73-fips; /run/mnt/kernel/kernel.efi	5.15.0-73-fips	N/A	HMAC SHA-512
*.ko files in /usr/lib/modules/5.15.0-73- fips/kernel/crypto/; *.ko files in /usr/lib/modules/5.15.0-73- fips/kernel/arch/x86/crypto/; *.ko files in /usr/lib/modules/5.15.0-73- fips/kernel/arch/arm64/crypto/; *.ko files in /usr/lib/modules/5.15.0-73- fips/kernel/arch/s390/crypto/	5.15.0-73-fips	N/A	RSA signature verification
/usr/lib/*-linux- gnu/libkcapi.so.1.4.0; /usr/bin/sha512hmac	1.4.0- 1ubuntu0.1~Fips1	N/A	HMAC SHA-256 (/usr/lib/*-linux- gnu/libkcapi.so.1.4.0); HMAC SHA-512 (/usr/bin/sha512hmac)

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

Tested Module Identification – Hybrid Disjoint Hardware:

N/A for this module.

Tested Operational Environments - Software, Firmware, Hybrid:

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

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

© 2024 Canonical Ltd. / atsec information security.

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

Operating System	Hardware Platform	Processors	PAA/PAI	Hypervisor or Host OS	Version(s)
Ubuntu 22.04 LTS 64-bit	Amazon Web Services (AWS) c6g.metal	AWS Graviton2	No	N/A	5.15.0-73- fips
Ubuntu Core 22 64-bit	Amazon Web Services (AWS) c6g.metal	AWS Graviton2	Yes	N/A	5.15.0-73- fips
Ubuntu Core 22 64-bit	Amazon Web Services (AWS) c6g.metal	AWS Graviton2	No	N/A	5.15.0-73- fips
Ubuntu 22.04 LTS 64-bit	IBM z15	IBM z15	Yes	N/A	5.15.0-73- fips
Ubuntu 22.04 LTS 64-bit	IBM z15	IBM z15	No	N/A	5.15.0-73- fips

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

Vendor-Affirmed Operational Environments - Software, Firmware, Hybrid: N/A for this module.

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

2.3 Excluded Components

Not applicable.

2.4 Modes of Operation

Modes List and	Description:
----------------	---------------------

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

Table 4: Modes List and Description

Mode Change Instructions and Status:

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

Degraded Mode Description:

Not applicable.

2.5 Algorithms

Approved Algorithms:

Algorithm	CAVP Cert	Reference
AES-ECB	A3812	SP 800-38A
Counter DRBG	A3812	SP 800-90A Rev. 1
Hash DRBG	A3812	SP 800-90A Rev. 1
HMAC DRBG	A3812	SP 800-90A Rev. 1
HMAC-SHA-1	A3812	FIPS 198-1
HMAC-SHA2-224	A3812	FIPS 198-1
HMAC-SHA2-256	A3812	FIPS 198-1
HMAC-SHA2-384	A3812	FIPS 198-1
HMAC-SHA2-512	A3812	FIPS 198-1
KAS-FFC-SSC Sp800-56Ar3	A3812	SP 800-56A Rev. 3
Safe Primes Key Generation	A3812	SP 800-56A Rev. 3
SHA-1	A3812	FIPS 180-4
SHA2-224	A3812	FIPS 180-4
SHA2-256	A3812	FIPS 180-4
SHA2-384	A3812	FIPS 180-4
SHA2-512	A3812	FIPS 180-4
AFS-FCB	A3813	SP 800-38A
Counter DRBG	A3813	SP 800-90A Rev. 1
FCDSA KeyGen (FIPS186-4)	A3813	FIPS 186-4
Hash DRBG	A3813	SP 800-90A Rev. 1
HMAC DRBG	A3813	SP 800-90A Rev. 1
HMAC-SHA-1	A3813	FIPS 198-1
HMAC-SHA2-224	A3813	FIPS 198-1
HMAC-SHA2-256	A3813	FIPS 198-1
HMAC-SHA2-384	A3813	FIPS 198-1
HMAC-SHA2-512	A3813	FIPS 198-1
KAS-ECC-SSC Sp800-56Ar3	A3813	SP 800-56A Rev. 3
SHA-1	A3813	FIPS 180-4
SHA2-224	A3813	FIPS 180-4
SHA2-256	A3813	FIPS 180-4
SHA2-384	A3813	FIPS 180-4
SHA2-512	A3813	FIPS 180-4
AES-CBC	A3814	SP 800-38A
AES-CCM	A3814	SP 800-38C
AES-CMAC	A3814	SP 800-38B
AES-CTR	A3814	SP 800-38A
AES-ECB	A3814	SP 800-38A
AES-GCM	A3814	SP 800-38D
AES-GMAC	A3814	SP 800-38D
AES-XTS Testing Revision 2.0	A3814	SP 800-38E
Counter DRBG	A3814	SP 800-90A Rev. 1
Hash DRBG	A3814	SP 800-90A Rev. 1
HMAC DRBG	A3814	SP 800-90A Rev. 1
HMAC-SHA-1	A3814	FIPS 198-1
HMAC-SHA2-224	A3814	FIPS 198-1
HMAC-SHA2-256	A3814	FIPS 198-1
HMAC-SHA2-384	A3814	FIPS 198-1
HMAC-SHA2-512	A3814	FIPS 198-1

Algorithm	CAVP Cert	Reference
RSA SigVer (FIPS186-4)	A3814	FIPS 186-4
SHA-1	A3814	FIPS 180-4
SHA2-224	A3814	FIPS 180-4
SHA2-256	A3814	FIPS 180-4
SHA2-384	A3814	FIPS 180-4
SHA2-512	A3814	FIPS 180-4
AES-KW	A3815	SP 800-38F
HMAC-SHA3-224	A3816	FIPS 198-1
HMAC-SHA3-256	A3816	FIPS 198-1
HMAC-SHA3-384	A3816	FIPS 198-1
HMAC-SHA3-512	A3816	FIPS 198-1
SHA3-224	A3816	FIPS 202
SHA3-256	A3816	FIPS 202
SHA3-384	A3816	FIPS 202
SHA3-512	A3816	FIPS 202
AES-CFB128	A3817	SP 800-38A
AES-OFB	A3818	SP 800-38A
AES-CBC-CS3	A3819	SP 800-38A
AES-ECB	A3820	SP 800-38A
AES-GCM	A3820	SP 800-38D
Counter DRBG	A3820	SP 800-90A Rev. 1
Hash DRBG	A3820	SP 800-90A Rev. 1
HMAC DRBG	A3820	SP 800-90A Rev. 1
AES-ECB	A3821	SP 800-38A
AES-GCM	A3821	SP 800-38D
Counter DRBG	A3821	SP 800-90A Rev. 1
Hash DRBG	A3821	SP 800-90A Rev. 1
HMAC DRBG	A3821	SP 800-90A Rev. 1
AES-CBC	A3822	SP 800-38A
AES-CCM	A3822	SP 800-38C
AES-CMAC	A3822	SP 800-38B
AES-CTR	A3822	SP 800-38A
AES-ECB	A3822	SP 800-38A
AES-GCM	A3822	SP 800-38D
AES-GMAC	A3822	SP 800-38D
AES-XTS Testing Revision 2.0	A3822	SP 800-38E
Counter DRBG	A3822	SP 800-90A Rev. 1
Hash DRBG	A3822	SP 800-90A Rev. 1
HMAC DRBG	A3822	SP 800-90A Rev. 1
AES-KW	A3823	SP 800-38F
AES-ECB	A3824	SP 800-38A
AES-GCM	A3824	SP 800-38D
Counter DRBG	A3824	SP 800-90A Rev. 1
Hash DRBG	A3824	SP 800-90A Rev. 1
HMAC DRBG	A3824	SP 800-90A Rev. 1
AES-ECB	A3825	SP 800-38A
AES-GCM	A3825	SP 800-38D
Counter DRBG	A3825	SP 800-90A Rev. 1
Hash DRBG	A3825	SP 800-90A Rev. 1
HMAC DRBG	A3825	SP 800-90A Rev. 1
AES-CFB128	A3826	SP 800-38A
AFS-OFB	A3827	SP 800-384

Algorithm	CAVP Cert	Reference
AES-CBC-CS3	A3828	SP 800-38A
AES-CBC	A3829	SP 800-38A
AES-CCM	A3829	SP 800-38C
AES-CMAC	A3829	SP 800-38B
AES-CTR	A3829	SP 800-38A
AES-ECB	A3829	SP 800-38A
AES-GCM	A3829	SP 800-38D
AES-GMAC	A3829	SP 800-38D
AES-XTS Testing Revision 2.0	A3829	SP 800-38E
Counter DRBG	A3829	SP 800-90A Rev. 1
AES-ECB	A3830	SP 800-38A
AES-GCM	A3830	SP 800-38D
Counter DRBG	A3830	SP 800-90A Rev. 1
Hash DRBG	A3830	SP 800-90A Rev. 1
HMAC DRBG	A3830	SP 800-90A Rev. 1
AES-ECB	A3831	SP 800-38A
AES-GCM	A3831	SP 800-38D
Counter DRBG	A3831	SP 800-90A Rev. 1
Hash DRBG	A3831	SP 800-90A Rev. 1
HMAC DRBG	A3831	SP 800-90A Rev. 1
AES-CBC	A3832	SP 800-38A
AES-CCM	A3832	SP 800-38C
AES-CMAC	A3832	SP 800-38B
AES-CTR	A3832	SP 800-38A
AES-ECB	A3832	SP 800-38A
AES-GCM	A3832	SP 800-38D
AES-GMAC	A3832	SP 800-38D
AES-XTS Testing Revision 2.0	A3832	SP 800-38E
Counter DRBG	A3832	SP 800-90A Rev. 1
Hash DRBG	A3832	SP 800-90A Rev. 1
HMAC DRBG	A3832	SP 800-90A Rev. 1
HMAC-SHA-1	A3832	FIPS 198-1
HMAC-SHA2-224	A3832	FIPS 198-1
HMAC-SHA2-256	A3832	FIPS 198-1
HMAC-SHA2-384	A3832	FIPS 198-1
HMAC-SHA2-512	A3832	FIPS 198-1
RSA SigVer (FIPS186-4)	A3832	FIPS 186-4
SHA-1	A3832	FIPS 180-4
SHA2-224	A3832	FIPS 180-4
SHA2-256	A3832	FIPS 180-4
SHA2-384	A3832	FIPS 180-4
SHA2-512	A3832	FIPS 180-4
AFS-FCB	A3833	SP 800-38A
AFS-GCM	Δ3833	SP 800-38D
	Δ3833	SP 800-904 Rev 1
Hash DRBG	Δ3833	SP 800-904 Rev. 1
	A3833	SP 800-90A Rev. 1
AFS-FCB	Δ3834	SP 800-384
AFS-GCM	Δ3834	SP 800-38D
	Δ3834	SD 800-900 Dav 1
Hach DRBC	Δ383/	SD 800-00A Rev. 1
		51 000-30A REV. 1

Algorithm	CAVP Cert	Reference
AES-KW	A3835	SP 800-38F
AES-CFB128	A3836	SP 800-38A
AES-OFB	A3837	SP 800-38A
AES-CBC-CS3	A3838	SP 800-38A
HMAC-SHA3-224	A3839	FIPS 198-1
HMAC-SHA3-256	A3839	FIPS 198-1
HMAC-SHA3-384	A3839	FIPS 198-1
HMAC-SHA3-512	A3839	FIPS 198-1
SHA3-224	A3839	FIPS 202
SHA3-256	A3839	FIPS 202
SHA3-384	A3839	FIPS 202
SHA3-512	A3839	FIPS 202
AES-CBC	A3840	SP 800-38A
AES-CTR	A3840	SP 800-38A
AES-ECB	A3840	SP 800-38A
AES-GCM	A3840	SP 800-38D
AFS-XTS Testing Revision 2.0	A3840	SP 800-38E
Counter DRBG	A3840	SP 800-90A Rev. 1
Hash DRBG	A3840	SP 800-90A Rev. 1
HMAC DRBG	A3840	SP 800-90A Rev. 1
AFS-FCB	A3841	SP 800-38A
AFS-GCM	A 3841	SP 800-38D
	A3841	SP 800-904 Rev 1
Hash DRBG	A 3841	SP 800-90A Rev. 1
	Δ3841	SP 800-904 Rev. 1
AFS-FCB	Δ3842	SP 800-384
AFS-GCM	Δ3842	SP 800-38D
	Δ3842	SP 800-904 Rev 1
Hash DRBG	Δ3842	SP 800-904 Rev. 1
	Δ3842	SP 800-904 Rev. 1
AFS-CBC	Δ3843	SP 800-384
AES-CCM	Δ3843	SP 800-38C
	A3843	SP 800-38B
	A3843	SP 800-384
	A38/3	SP 800-38A
AES-CCM	A38/3	SP 800-38D
	A3943	SP 800-38D
AES-YTS Testing Povision 2.0	A 3 9 4 3	SD 800-38E
Counter DBBC	A3043	SP 800-38L SP 800-90A Dov 1
	A3043	SP 800-90A Rev. 1
	A3043	SP 800-90A Rev. 1
	A 3043	CD 000 20A REV. 1
	A3044 A2011	
	A3044	SP 800-380
	A3844	SP 800-90A Rev. 1
	A3844	SP 800-90A Rev. 1
	A3844	SP 800-90A Rev. 1
AES-ECB	A3845	SP 800-38A
	A 3045	57 800-38D
	A 3845	SP 800-90A Rev. 1
	A3845	57 800-90A Rev. 1
	A3845	5P 800-90A Rev. 1
IAES-KW	A3846	SP 800-38F

Algorithm	CAVP Cert	Reference
AES-CFB128	A3847	SP 800-38A
AES-OFB	A3848	SP 800-38A
AES-CBC-CS3	A3849	SP 800-38A
Hash DRBG	A3850	SP 800-90A Rev. 1
HMAC DRBG	A3850	SP 800-90A Rev. 1
HMAC-SHA-1	A3850	FIPS 198-1
HMAC-SHA2-224	A3850	FIPS 198-1
HMAC-SHA2-256	A3850	FIPS 198-1
HMAC-SHA2-384	A3850	FIPS 198-1
HMAC-SHA2-512	A3850	FIPS 198-1
RSA SigVer (FIPS186-4)	A3850	FIPS 186-4
SHA-1	A3850	FIPS 180-4
SHA2-224	A3850	FIPS 180-4
SHA2-256	A3850	FIPS 180-4
SHA2-384	A3850	FIPS 180-4
SHA2-512	A3850	FIPS 180-4
Hash DRBG	A3851	SP 800-90A Rev. 1
HMAC DRBG	A3851	SP 800-90A Rev. 1
HMAC-SHA-1	A3851	FIPS 198-1
HMAC-SHA2-224	A3851	FIPS 198-1
HMAC-SHA2-256	A3851	FIPS 198-1
HMAC-SHA2-384	A3851	FIPS 198-1
HMAC-SHA2-512	A3851	FIPS 198-1
RSA SigVer (FIPS186-4)	A3851	FIPS 186-4
SHA-1	A3851	FIPS 180-4
SHA2-224	A3851	FIPS 180-4
SHA2-256	A3851	FIPS 180-4
SHA2-384	A3851	FIPS 180-4
SHA2-512	A3851	FIPS 180-4
Hash DRBG	A3852	SP 800-90A Rev. 1
HMAC DRBG	A3852	SP 800-90A Rev. 1
HMAC-SHA-1	A3852	FIPS 198-1
HMAC-SHA2-224	A3852	FIPS 198-1
HMAC-SHA2-256	A3852	FIPS 198-1
HMAC-SHA2-384	A3852	FIPS 198-1
HMAC-SHA2-512	A3852	FIPS 198-1
RSA SigVer (FIPS186-4)	A3852	FIPS 186-4
SHA-1	A3852	FIPS 180-4
SHA2-224	A3852	FIPS 180-4
SHA2-256	A3852	FIPS 180-4
SHA2-384	A3852	FIPS 180-4
SHA2-512	A3852	FIPS 180-4
AFS-CBC	A3853	SP 800-38A
AFS-CBC-CS3	A3853	SP 800-38A
AFS-CCM	Δ3853	SP 800-38C
AFS-CMAC	A3853	SP 800-38B
AFS-CTR	Δ3853	SP 800-384
AFS-FCB	Δ3853	SP 800-384
AFS-XTS Testing Revision 20	A3853	SP 800-38F
HMAC-SHA-1	Δ3853	FIPS 198-1
ΗΜΔC-SHΔ2-224	Δ3853	FIPS 198-1
ΗΜΔC-SHΔ2-256	Δ3853	FIPS 198-1

Algorithm	CAVP Cert	Reference
SHA-1	A3853	FIPS 180-4
SHA2-224	A3853	FIPS 180-4
SHA2-256	A3853	FIPS 180-4
AES-CBC	A3854	SP 800-38A
AES-CBC-CS3	A3854	SP 800-38A
AES-CCM	A3854	SP 800-38C
AES-CFB128	A3854	SP 800-38A
AES-CMAC	A3854	SP 800-38B
AES-CTR	A3854	SP 800-38A
AES-ECB	A3854	SP 800-38A
AES-GCM	A3854	SP 800-38D
AES-GMAC	A3854	SP 800-38D
AES-KW	A3854	SP 800-38F
AES-OFB	A3854	SP 800-38A
AES-XTS Testing Revision 2.0	A3854	SP 800-38E
Counter DRBG	A3854	SP 800-90A Rev. 1
AES-ECB	A3855	SP 800-38A
AES-GCM	A3855	SP 800-38D
Counter DRBG	A3855	SP 800-90A Rev. 1
Hash DRBG	A3855	SP 800-90A Rev. 1
HMAC DRBG	A3855	SP 800-90A Rev. 1
AES-ECB	A3856	SP 800-38A
AES-GCM	A3856	SP 800-38D
Counter DRBG	A3856	SP 800-90A Rev. 1
Hash DRBG	A3856	SP 800-90A Rev. 1
HMAC DRBG	A3856	SP 800-90A Rev. 1
AES-CBC	A3857	SP 800-38A
AES-CTR	A3857	SP 800-38A
AES-ECB	A3857	SP 800-38A
AES-XTS Testing Revision 2.0	A3857	SP 800-38E
HMAC-SHA2-224	A3857	FIPS 198-1
HMAC-SHA2-256	A3857	FIPS 198-1
SHA2-224	A3857	FIPS 180-4
SHA2-256	A3857	FIPS 180-4
HMAC-SHA2-224	A3858	FIPS 198-1
HMAC-SHA2-256	A3858	FIPS 198-1
HMAC-SHA2-384	A3858	FIPS 198-1
HMAC-SHA2-512	A3858	FIPS 198-1
SHA2-224	A3858	FIPS 180-4
SHA2-256	A3858	FIPS 180-4
SHA2-384	A3858	FIPS 180-4
SHA2-512	A3858	FIPS 180-4

Table 5: Approved Algorithms

Vendor-Affirmed Algorithms:

Name	Properties	Implementation	Reference
ECC and	Key Type:Asymmetric	N/A	SP800-133r2, section
DH CKG	ECC Curves:P-256, P-384 (strength of 128, 192		4 (without XOR)
	bits)		
	DH groups:ffdhe2048, ffdhe3072, ffdhe4096,		
	ffdhe6144, ffdhe8192 (strength of 112-200 bits)		

Table 6: Vendor-Affirmed Algorithms

ubuntu[©]Canonical Ltd. Ubuntu 22.04 Kernel Crypto API Cryptographic Module FIPS 140-3 Non-Proprietary Security Policy

Non-Approved, Allowed Algorithms:

N/A for this module.

Non-Approved, Allowed Algorithms with No Security Claimed:

N/A for this module.

Non-Approved, Not Allowed Algorithms:

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

Table 7: Non-Approved, Not Allowed Algorithms

2.6 Security Function Implementations

Name	Туре	Description	Properties	Algorithms
Encryption and	BC-UnAuth	SP800-38A.	AES-ECB keys:128,	AES-ECB
Decryption with		Encryption,	192, 256 bits with	AES-ECB
AES		Decryption; SP800-	128, 192, 256 bits	AES-ECB
		38F. KTS (key	of strength	AES-ECB
		wrapping and key	AES-CBC keys:128,	AES-ECB
		unwrapping) per IG	192, 256 bits with	AES-ECB
		D.G	128, 192, 256 bits	AES-ECB
			of strength	AES-ECB
			AES-CTR keys:128,	AES-ECB
			192, 256 bits with	AES-ECB
			128, 192, 256 bits	AES-ECB
			of strength	AES-ECB
			AES-XTS Testing	AES-ECB
			Revision 2.0	AES-ECB
			keys:128, 256 bits	AES-ECB
			with 128 and 256	AES-ECB
			bits of strength	AES-ECB
			AES-KW keys:128,	AES-ECB
			192, 256 bits with	AES-ECB
			128, 192, 256 bits	AES-ECB
			of strength	AES-ECB
			AES-CFB128	AES-ECB
			keys:128, 192, 256	AES-ECB
			bits with 128, 192,	AES-ECB
			256 bits of strength	AES-ECB
			AES-OFB keys:128,	AES-CBC
			192, 256 bits with	AES-CBC
			128, 192, 256 bits	AES-CBC
			of strength	AES-CBC
			AES-CBC-CS3	AES-CBC

© 2024 Canonical Ltd. / atsec information security.

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

Name	Туре	Description	Properties	Algorithms
			keys:128, 192, 256	AES-CBC
			bits with 128, 192,	AES-CBC
			256 bits of strength	AES-CBC
				AES-CBC
				AES-CTR
				AES-CIR
				AES-CIR
				AES-XIS lesting
				REVISION 2.0
				AES-ATS Tesuing
				AES VIS Tocting
				ALS-ATS TESUING
				AES_YTS Tecting
				Pevision 2.0
				AFS-XTS Testing
				Revision 2.0
				AFS-XTS Testing
				Revision 2.0
				AES-XTS Testing
				Revision 2.0
				AES-XTS Testing
				Revision 2.0
				AES-XTS Testing
				Revision 2.0
				AES-KW
				AES-CFB128
				AES-CFB128
				AES-CFB128
				AES-CEB120
				AES-CFB128
				AFS-OFR
				AFS-OFB
				AFS-OFB
				AES-CBC-CS3
Random Number	DRBG	SP800-90Ar1.	Counter DRBG:128,	Counter DRBG
Generation with		Random number	192, 256 bits	Counter DRBG
HMAC DRBG. Hash		generation	HMAC DRBG:128.	Counter DRBG

Name	Туре	Description	Properties	Algorithms
DRBG or Counter			256 bits	Counter DRBG
DRBG			Hash DRBG:128,	Counter DRBG
			256 bits	Counter DRBG
				HMAC DRBG
				HMAC DRBG
				HMAC DRBG
				HMAC DRBG
				HMAC DRBG
				HMAC DRBG
				HMAC DRBG
				HMAC DRBG
				HMAC DRBG
				HMAC DRBG
				HMAC DRBG
				HMAC DRBG
				HMAC DRBG
				HMAC DRBG
				HMAC DRBG
				HMAC DRBG
				HMAC DRBG
				HMAC DRBG
				HMAC DRBG
				HMAC DRBG
				HMAC DRBG
				HMAC DRBG
				HMAC DRBG
				HMAC DRBG
				Hash DRBG

Message MAC SP800-388, SP800- Hash DRBG Hash HAG SHA-12 HAG SHA-12 HMAC SHA-22 HAS HMAC SHA-22 HAS HMAC SHA-22 HAS HMAC SHA-22 HAS HMAC SHA-224 HMAC SHA-2256 HMAC SHA-224 HMAC SHA-2256 HMAC SHA-224 HMAC SHA-2256 HMAC SH	Name	Туре	Description	Properties	Algorithms
Message MAC SP800-388, SP800- Hash DR8G Hash DR8G HAS HMAC SHA1 HMAC SHA1 HMAC SHA2 HAS HMAC SHA1 HMAC SHA2 224 HMAC					Hash DRBG
Message Authentication with AES or HMAC Mass DRBG Mass DRBG MAC SHA1 MMAC SHA2 Mass SHA1 MAC SHA2 Mass SHA1 MAC SHA2 Mass SHA2 MAC SHA2 Mass SHA2 MAC SHA2					Hash DRBG
Message Authentication with AES or HMACMACSP800-388, SP800- Mash DR8G Hash DR8G HAC-SHA-1Message authentication tis sits of strength HMAC-SHA-2248 HMAC-SHA-1 bits vith 112-256 bits with 112-256 bits with 112-256 bits with 112-256 bits with 112-256 HMAC-SHA-2224 HMAC-SHA-2226 HMAC-SHA-2224 HMAC-SHA-2226 HMAC-SHA-2226 HMAC-SHA-2226 HMAC-SHA-2226 HMAC-SHA-2266 HMAC-SHA					Hash DRBG
MessageMACSP800-38B, SP800-HMAC-SHA-1Hash DRBGMessageMACSP800-38B, SP800-HMAC-SHA-1HMAC-SHA-1Authentication with AES or HMAC38D, FISP198-1. Messagekeys:112-524288HMAC-SHA-1MACS-SHA-1MAC-SHA-1keys:112-524288HMAC-SHA-1MMACMacsHMAC-SHA-1keys:112-524288HMAC-SHA-1Macs-SHA-1Messagebits of strengthHMAC-SHA-1bits of strengthHMAC-SHA-224HMAC-SHA-224HMAC-SHA-224HMAC-SHA-224HMAC-SHA-224bits of strengthHMAC-SHA-224HMAC-SHA-2256HMAC-SHA-224HMAC-SHA-224HMAC-SHA-224HMAC-SHA-224HMAC-SHA-224HMAC-SHA-224HMAC-SHA-224HMAC-SHA-224HMAC-SHA-224HMAC-SHA-224HMAC-SHA-224HMAC-SHA-224HMAC-SHA-224HMAC-SHA-224HMAC-SHA-224HMAC-SHA-224HMAC-SHA-224HMAC-SHA-224HMAC-SHA-224HMAC-SHA-2256HMAC-SHA-2256HMAC-SHA-2256HMAC-SHA-2256HMAC-SHA-2256HMAC-SHA-2256HMAC-SHA-2256HMAC-SHA-2256HMAC-SHA-2256HMAC-SHA-2256HMAC-SHA-2256HMAC-SHA-226HMAC-SHA-2256HMAC-SHA-226HMAC-SHA-256HMAC-SHA-226HMAC-SHA-256HMAC-SHA-226HMAC-SHA-256HMAC-SHA-226HMAC-SHA-256HMAC-SHA-226HMAC-SHA-256HMAC-SHA-226HMAC-SHA-256HMAC-SHA-226HMAC-SHA-256HMAC-SHA-226<					Hash DRBG
Message Authentication with AES or HMACMACSP800-388, SP800- Hash DR8G Hash DR8G HAACSHA-11 HMAC-SHA-12248 HMAC-SHA-14 HMAC-SHA-2244 HMAC-SHA-14 HMAC-SHA-2244 HMAC-SHA-14 HMAC-SHA-2244 HMAC-SHA-1256 HMAC-SHA-14 HMAC-SHA-2246 HMAC-SHA-2244 HMAC-SHA-2246 HMAC-SHA-2246 HMAC-SHA-2246 HMAC-SHA-2246 HMAC-SHA-2246 HMAC-SHA-2246 HMAC-SHA-2246 HMAC-SHA-2246 HMAC-SHA-2246 HMAC-SHA-2246 HMAC-SHA-2246 HMAC-SHA-2246 HMAC-SHA-2246 HMAC-SHA-2246 HMAC-SHA-2246 HMAC-SHA-2256 HMAC-S					Hash DRBG
Message Authentication with AES or HMACMACSP800-388, SP800- Hash DR8G Hash DR8G HAACSHA-1Message authentication with AES or HMACMACSHA-11 Keys:112-524288 HMAC-SHA-1 bits with 112-256 HMAC-SHA-1 HMAC-SHA-224 HMAC-SHA-1 with 112-256 bits of HMAC-SHA-1 HMAC-SHA-224 HMAC-SHA-224 HMAC-SHA-1 HMAC-SHA-224 HMAC-SHA-2256 HMAC-SHA-2256 HMAC-SHA-2256 HMAC-SHA-2256 HMAC-SHA-2256 HMAC-SHA-2256 HMAC-SHA-2256 HMAC-SHA-2256 HMAC-SHA-2256 HMAC-SHA-2256 HMAC-SHA-2256 HMAC-SHA-2256 HMAC-SHA-2256 HMAC-SHA-2256 HMAC-SHA-2256 HMAC-SHA-2256 HMAC-SHA-2256 HMAC-SHA-2264 HMAC-SHA-2256 HMAC-SHA-2264 HMAC-SHA-2264 HMAC-SHA-2264 HMAC-SHA-2264 HMAC-SHA-2266 HMAC-SHA-2264 HMAC-SHA-2266 <b< td=""><td></td><td></td><td></td><td></td><td>Hash DRBG</td></b<>					Hash DRBG
Message Authentication with AES or HMAC Authentication with AES or HMAC Message authentication MAC Message MAC Message MAC Message MAC Message MAC Message MAC Message MAC Message MAC Message MAC Message MAC Message MAC Message MAC Message MAC MAC MAC MAC MAC MAC MAC MAC					Hash DRBG
Message Authentication with AES or HMAC Mac Mac Mac Mac Mac Mac Mac Mac					Hash DRBG
Message Authentication with AES or HMAC AES or HMAC MAC Message authentication MAC Message MAC Message MAC Message MAC Message MAC Message MAC Message MAC Message MAC Message MAC MACSHA-1 HMACSHA-224 HMACSHA-2248 HMACSHA-1 HMACSHA-2248 HMACSHA-1 HMACSHA-2248 HMACSHA-2248 HMACSHA-2248 HMACSHA-2248 HMACSHA-2248 HMACSHA-2248 HMACSHA-2248 HMACSHA-2248 HMACSHA-2248 HMACSHA-2248 HMACSHA-2248 HMACSHA-2248 HMACSHA-2248 HMACSHA-2248 HMACSHA-2248 HMACSHA-2248 HMACSHA-2248 HMACSHA-2248 HMACSHA-2248 HMACSHA-2224 HMACSHA-2248 HMACSHA-2224 HMACSHA-2248 HMACSHA-2224 HMACSHA-2248 HMACSHA-2224 HMACSHA-2248 HMACSHA-2224 HMACSHA-2224 HMACSHA-2224 HMACSHA-2224 HMACSHA-2224 HMACSHA-2224 HMACSHA-2226 HMACSHA-2226 HMACSHA-2226 HMACSHA-2226 HMACSHA-2226 HMACSHA-2256 HMACSHA-					Hash DRBG
MACSP800-388, SP800- 380, FISP198-1. Message authentication with AES or HMACMACSP800-388, SP800- HMAC-SHA-1 bits with 112-254288 bits of strength HMAC-SHA-1 HMAC-SHA-1 HMAC-SHA-1 HMAC-SHA-1 HMAC-SHA-1 HMAC-SHA-1 HMAC-SHA-1 HMAC-SHA-1 HMAC-SHA-1 HMAC-SHA-1 HMAC-SHA-1 HMAC-SHA-1224 HMAC-SHA-1 HMAC-SHA-1256 bits HMAC-SHA-13 HMAC-SHA-224 HMAC-SHA-224 HMAC-SHA-224 HMAC-SHA-224 HMAC-SHA-224 HMAC-SHA-224 HMAC-SHA-224 HMAC-SHA-224 HMAC-SHA-224 HMAC-SHA-224 HMAC-SHA-224 HMAC-SHA-224 HMAC-SHA2-224 HMAC-SHA2-224 HMAC-SHA2-224 HMAC-SHA2-224 HMAC-SHA2-224 HMAC-SHA2-224 HMAC-SHA2-224 HMAC-SHA2-224 HMAC-SHA2-224 HMAC-SHA2-224 HMAC-SHA2-224 HMAC-SHA2-224 HMAC-SHA2-224 HMAC-SHA2-224 HMAC-SHA2-224 HMAC-SHA2-224 HMAC-SHA2-224 HMAC-SHA2-226 bits of strength HMAC-SHA2-226 bits of strength HMAC-SHA2-226 HMAC-SHA2-2384 HMAC-SHA2-2384 HMAC-SHA2-384 HMAC-SHA2-384 HMAC-SHA2-384 HMAC-SHA2-384 HMAC-SHA2-384 HMAC-SHA2-384 HMAC-SHA2-312 HMAC-SHA2-312 HMAC-SHA2-312 HMAC-SHA2-312 HMAC-SHA2-312 HMAC-SHA2-312 HMAC-SHA2-312 HMAC-SHA2-312 HMAC-SHA2-312 HMAC-SHA2-312 HMAC-SHA2-312 HMAC-SHA2-312 HMAC-SHA2-312 HMAC-SHA2-312 HMAC-SHA					Hash DRBG
Massage Authentication with AES or HMACMACSP800-38B, SP800- 38D, FISP198-1. Keys:112-52428BHMAC-SHA-1 HMAC-SHA-1AES or HMACMACBAD, FISP198-1. Message authenticationHits with 112-256HMAC-SHA-1 HMAC-SHA-1MESSage authenticationHMAC-SHA-1 bits of strengthHMAC-SHA-1 HMAC-SHA-1HMAC-SHA-1 With 112-256 bits of bits of strengthHMAC-SHA-1 HMAC-SHA-2224 HMAC-SHA-2284HMAC-SHA2-224 HMAC-SHA2-224HMAC-SHA2-224 HMAC-SHA2-224 bits of strengthHMAC-SHA2-224 HMAC-SHA2-224HMAC-SHA2-224 bits of strengthHMAC-SHA2-224 bits of strengthHMAC-SHA2-224 HMAC-SHA2-224HMAC-SHA2-224 bits of strengthHMAC-SHA2-224 HMAC-SHA2-224HMAC-SHA2-224 bits of strengthHMAC-SHA2-224 HMAC-SHA2-224 HMAC-SHA2-2256HMAC-SHA2-226 bits with 112-256HMAC-SHA2-226 HMAC-SHA2-2256HMAC-SHA2-226 bits with 1128, 192, HMAC-SHA2-2256 bits with 1128, 192, HMAC-SHA2-2256 HMAC-SHA2-2256HMAC-SHA2-226 bits with 1128, 192, HMAC-SHA2-2256 bits with 1128, 192, HMAC-SHA2-236 HMAC-SHA2-236HMAC-SHA2-236 HMAC-SHA2-236HMAC-SHA2-236 HMAC-SHA2-236HMAC-SHA2-236 HMAC-SHA2-236HMAC-SHA2-2384 HMAC-SHA2-236HMAC-SHA2-236 HMAC-SHA2-2384 HMAC-SHA2-384HMAC-SHA2-384 HMAC-SHA2-384 HMAC-SHA2-384HMAC-SHA2-384 HMAC-SHA2-384 HMAC-SHA2-384 HMAC-SHA2-384 HMAC-SHA2-384 HMAC-SHA2-384 HMAC-SHA2-384 HMAC-SHA2-384 HMAC-SHA2-384 HMAC-SHA2-384 HMAC-SHA2-384 HMAC-SHA2-384 HMAC-SHA2-384 HMAC-SHA2-384 HMAC-SHA2-384 <td></td> <td></td> <td></td> <td></td> <td>Hash DRBG</td>					Hash DRBG
MAC Authentication with AES or HMAC AES or HMAC AES or HMAC} HMAC HAC HAC HAC H					Hash DRBG
Message Authentication with AES or HMACMACSP800-388, SP800 380, FISP198-1. Message authenticationHMAC-SHA-1 HMAC-SHA-1 bits of strength HMAC-SHA-1 HMAC-SHA-1 HMAC-SHA-1 HMAC-SHA-1 HMAC-SHA-1 HMAC-SHA-1 HMAC-SHA-1 HMAC-SHA-1 With 112-256 HMAC-SHA-1 HMAC-SHA-1 HMAC-SHA-1 HMAC-SHA-1 HMAC-SHA-1 HMAC-SHA-1 HMAC-SHA-1 HMAC-SHA-1 HMAC-SHA-224 HMAC-SHA-1 HMAC-SHA-224 HMAC-SHA-224 HMAC-SHA-224 HMAC-SHA2-226 HMAC-SHA2-2384 HMAC-SHA2-2384 HMAC-SHA2-384 HMAC-SHA2-384 HMAC-SHA2-384 HMAC-SHA2-384 HMAC-SHA2-384 HMAC-SHA2-384 HMAC-SHA2-384 HMAC-SHA2-384 HMAC-SHA2-384 HMAC-SHA2-384 HMAC-SHA2-384 HMAC-SHA2-384 HMAC-SHA2-384 HMAC-SHA2-384 HMAC-SHA2-384 HMAC-SHA2-512 HMAC-SHA2-512 HMAC-SHA2-512 HMAC-SHA2-512 HMAC-SHA2-512 HMAC-SHA2-512 HMAC-SHA2-512 HMAC-SHA2-512 HMAC-SHA2-512 HMAC-SHA2-512 HMAC-SHA2-512 HMAC-SHA2-512 <td></td> <td></td> <td></td> <td></td> <td>Hash DRBG</td>					Hash DRBG
Authentication 38D, FISP198-1. keys:112-52428 HMAC-SHA-1 AES or HMAC Message bits with 112-256 HMAC-SHA-1 authentication bits of strength HMAC-SHA-1 HMAC-SHA-2224 HMAC-SHA-1 keys:112-524288 HMAC-SHA-1 bits of strength HMAC-SHA-2224 HMAC-SHA-2224 HMAC-SHA-2224 HMAC-SHA2-224 HMAC-SHA2-224 HMAC-SHA2-224 HMAC-SHA2-224 HMAC-SHA2-2288 HMAC-SHA2-224 HMAC-SHA2-2248 HMAC-SHA2-224 bits of strength HMAC-SHA2-226 bits of strength HMAC-SHA2-226 bits of strength HMAC-SHA2-226 bits of strength HMAC-SHA2-226	Message	MAC	SP800-38B, SP800-	HMAC-SHA-1	HMAC-SHA-1
AES or HMAC Message bits with 112-256 HMAC-SHA-1 authentication bits of strength HMAC-SHA-1 HMAC-SHA2-224 HMAC-SHA-1 keys:112-524288 HMAC-SHA-1 bits 112-256 bits of MAC-SHA-1 bits 112-256 bits of MAC-SHA-1 with 112-256 HMAC-SHA2-224 HMAC-SHA2-2256 HMAC-SHA2-224 HMAC-SHA2-226 HMAC-SHA2-224 bits of strength HMAC-SHA2-226 HMAC-SHA2-226 HMAC-SHA2-226 bits of strength HMAC-SHA2-226 bits of strength HMAC-SHA2-	Authentication with		38D, FISP198-1.	keys:112-524288	HMAC-SHA-1
authentication bits of strength HMAC-SHA-1 HMAC-SHA2-224 HMAC-SHA-1 keys:112-256 bits of HMAC-SHA-1 with 112-256 bits of HMAC-SHA-2224 HMAC-SHA2-2256 HMAC-SHA-2224 HMAC-SHA2-2256 HMAC-SHA2-224 HMAC-SHA2-2256 HMAC-SHA2-224 bits with 112-256 HMAC-SHA2-224 bits of strength HMAC-SHA2-224 bits with 112-256 HMAC-SHA2-224 bits of strength HMAC-SHA2-224 bits with 112-256 HMAC-SHA2-224 bits of strength HMAC-SHA2-226 bits of strength HMAC-SHA2-226 bits of strength HMAC-SHA2-226 bits of strength HMAC-SHA2-256 bits with 128, 192, 256 bits with 128, 192, 256 bits with 128, 192, HMAC-SHA2-256 bits with 128, 192, 256 bits with 128, 192, HMAC-SHA2-256 bits with 128, 192, 256 bits with 128, 192, 256 bits with 128, 192, 256 bits with 128, 192, 4MAC-SHA2-256 bits with 128, 192, 256 bits with 128, 192, 256 bits with 128, 192, 256 bits with 128, 2384 HMAC-SHA3-256 bits of strength HMAC-SHA2-256 bits with 112-256 HMAC-SHA2-2364 bits of strength HMAC-SHA2-2364 bits with 112-256 HMAC-SHA2-384 HMAC-SHA3-226 bits of strength HMAC-SHA2-384 HMAC-SHA3-226 bits of strength HMAC-SHA2-384 bits with 112-256 HMAC-SHA2-512 bits of strength HMAC-SHA2-512 bits of strength HMAC-SHA2-512 bits of strength HMAC-SHA2-512 bits of strength HMAC-SHA2-512	AES or HMAC		Message	bits with 112-256	HMAC-SHA-1
HMAC-SHA-224 HMAC-SHA-1 keys:112-524288 HMAC-SHA-1 bits bits strength HMAC-SHA-224 HMAC-SHA2-256 HMAC-SHA2-224 HMAC-SHA2-256 HMAC-SHA2-224 HMAC-SHA2-256 HMAC-SHA2-224 bits with bits of bits of strength HMAC-SHA2-224 bits of bits of strength HMAC-SHA2-224 bits of bits of bits of HMAC-SHA2-224 HMAC-SHA2-224 bits wits bits of bits of bits of HMAC-SHA2-224 HMAC-SHA2-224 bits mAC-SHA2-224 bits mAC-SHA2-224 HMAC-SHA2-226 HMAC-SHA2-226 bits of bits of bits of HMAC-SHA2-256 HMAC-SHA2-256 bits with L			authentication	bits of strength	HMAC-SHA-1
keys:112-524288 HMAC-SHA-1 bits 112-256 HMAC-SHA-1 with 112-256 HMAC-SHA-1 with 112-256 HMAC-SHA-1 strength HMAC-SHA2-224 HMAC-SHA2-256 HMAC-SHA2-224 keys:112-524288 HMAC-SHA2-224 bits with 112-256 HMAC-SHA2-224 bits of strength HMAC-SHA2-224 bits of strength HMAC-SHA2-224 bits with 112-256 HMAC-SHA2-224 bits with 112-256 HMAC-SHA2-224 bits with 112-256 HMAC-SHA2-224 bits of strength HMAC-SHA2-224 bits of strength HMAC-SHA2-224 HMAC-SHA2-512 HMAC-SHA2-226 bits of strength HMAC-SHA2-226 bits of strength HMAC-SHA2-256 bits with 112-256 HMAC-SHA2-256 bits of strength HMAC-SHA				HMAC-SHA2-224	HMAC-SHA-1
bits 112-256 bits of HMAC-SHA-1 with 112-256 bits of HMAC-SHA-224 HMAC-SHA2-224 keys:112-524288 HMAC-SHA2-224 bits of strength HMAC-SHA2-224 bits of strength HMAC-SHA2-224 keys:112-524288 HMAC-SHA2-224 bits with 112-256 HMAC-SHA2-224 bits of strength HMAC-SHA2-224 HMAC-SHA2-512 bits of strength HMAC-SHA2-226 bits of strength HMAC-SHA2-256 bits with 112-256 HMAC-SHA2-256 bits of strength HMAC-SHA2-256 bits of strength HMAC-SHA2-256 bits of strength HMAC-SHA2-256 bits of strength HMAC-SHA2-256 bits with 128, 192, JMAC-SHA2-256 bits of strength HMAC-SHA2-256 bits of strength HMAC-SHA2-384 HMAC-SHA3-324 HMAC-SHA3-384 HMAC-SH				keys:112-524288	HMAC-SHA-1
with 112-256 bits of HMAC-SHA-1 strength HMAC-SHA2-224 HMAC-SHA2-256 HMAC-SHA2-224 HMAC-SHA2-256 HMAC-SHA2-224 bits with 112-524288 HMAC-SHA2-224 bits of strength HMAC-SHA2-224 bits with 112-526 HMAC-SHA2-224 HMAC-SHA2-384 HMAC-SHA2-224 HMAC-SHA2-384 HMAC-SHA2-224 bits of strength HMAC-SHA2-224 bits with 112-256 HMAC-SHA2-224 bits of strength HMAC-SHA2-224 bits of strength HMAC-SHA2-224 bits of strength HMAC-SHA2-224 bits of strength HMAC-SHA2-224 HMAC-SHA2-512 HMAC-SHA2-224 HMAC-SHA2-512 HMAC-SHA2-224 HMAC-SHA2-512 HMAC-SHA2-224 HMAC-SHA2-512 HMAC-SHA2-224 HMAC-SHA2-512 HMAC-SHA2-224 HMAC-SHA2-224 HMAC-SHA2-224 HMAC-SHA2-512 HMAC-SHA2-224 HMAC-SHA2-512 HMAC-SHA2-226 bits with 112-256 HMAC-SHA2-256 Dits of strength HMAC-SHA2-256 <td></td> <td></td> <td></td> <td>bits 112-256 bits</td> <td>HMAC-SHA-1</td>				bits 112-256 bits	HMAC-SHA-1
strength HMAC-SHA2-224 HMAC-SHA2-256 HMAC-SHA2-224 HMAC-SHA2-256 HMAC-SHA2-224 bits with 112-526 HMAC-SHA2-224 bits of strength HMAC-SHA2-224 bits with 112-526 HMAC-SHA2-224 bits of strength HMAC-SHA2-224 bits of strength HMAC-SHA2-224 bits with 112-256 HMAC-SHA2-224 bits with 112-256 HMAC-SHA2-224 HMAC-SHA2-224 HMAC-SHA2-224 HMAC-SHA2-224 HMAC-SHA2-226 bits of strength HMAC-SHA2-226 bits of strength HMAC-SHA2-226 bits with 112-256 HMAC-SHA2-256 bits with 128, 192, 192, 256 HMAC-SHA2-256 bits with 128, 192, 194 HMAC-SHA2-256 bits with 128, 192, 194 HMAC-SHA2-256 bits with 112-524 HMAC-SHA2-384 HMAC-SHA2-384 HMAC-SHA2-384 <t< td=""><td></td><td></td><td></td><td>with 112-256 bits of</td><td>HMAC-SHA-1</td></t<>				with 112-256 bits of	HMAC-SHA-1
HMAC-SHA2-256 HMAC-SHA2-224 keys:112-524288 HMAC-SHA2-224 bits with 112-256 HMAC-SHA2-224 bits of strength HMAC-SHA2-224 HMAC-SHA2-384 HMAC-SHA2-224 HMAC-SHA2-384 HMAC-SHA2-224 keys:112-524288 HMAC-SHA2-224 bits of strength HMAC-SHA2-224 HMAC-SHA2-512 HMAC-SHA2-224 bits of strength HMAC-SHA2-256 bits with 112-256 HMAC-SHA2-256 bits with 112-256 HMAC-SHA2-256 bits with 128, 192, 256 HMAC-SHA2-256 bits with 128, 192, 256 HMAC-SHA2-256 bits with 128, 192, 256 HMAC-SHA2-356 HMAC-SHA3-224 HMAC-SHA2-356 HMAC-SHA3-224 HMAC-SHA2-384 HMAC-SHA3-224 HMAC-SHA2-384 HMAC-SHA3-3256 HMAC-SHA2-384 HMAC-SHA3-326 HMAC-SHA2-384 bits with 112-256 HMAC-SHA2-384 bits with 112-256<				strength	HMAC-SHA2-224
keys:112-524288 HMAC-SHA2-224 bits with 112-256 HMAC-SHA2-224 bits of strength HMAC-SHA2-224 HMAC-SHA2-224 HMAC-SHA2-224 HMAC-SHA2-224 HMAC-SHA2-224 bits with 112-256 HMAC-SHA2-224 bits of strength HMAC-SHA2-224 bits of strength HMAC-SHA2-224 HMAC-SHA2-512 HMAC-SHA2-224 HMAC-SHA2-512 HMAC-SHA2-224 HMAC-SHA2-512 HMAC-SHA2-224 HMAC-SHA2-512 HMAC-SHA2-224 HMAC-SHA2-512 HMAC-SHA2-224 HMAC-SHA2-512 HMAC-SHA2-224 HMAC-SHA2-226 HMAC-SHA2-256 bits with 112-56 HMAC-SHA2-256 bits of strength HMAC-SHA2-256 bits with 128, 192, 256 HMAC-SHA2-256 bits with 128, 192, 256 HMAC-SHA2-256 bits with 128, 192, 256 HMAC-SHA2-256 bits of strength HMAC-SHA2-384 HMAC-SHA2-226 HMAC-SHA2-384 bits with 112-256 HMAC-SHA2-384 bits with 112-256 HMAC-SHA2-384 bits of strength HMAC-SHA2-384 bits with 112-256 <td></td> <td></td> <td></td> <td>HMAC-SHA2-256</td> <td>HMAC-SHA2-224</td>				HMAC-SHA2-256	HMAC-SHA2-224
bits with 112-256 HMAC-SHA2-224 bits of strength HMAC-SHA2-224 HMAC-SHA2-384 HMAC-SHA2-224 keys:112-524288 HMAC-SHA2-224 bits with 112-256 HMAC-SHA2-224 HMAC-SHA2-512 HMAC-SHA2-224 Keys:112-524288 HMAC-SHA2-226 bits with 112-256 HMAC-SHA2-256 bits with 112-256 HMAC-SHA2-256 bits with 112, 256 HMAC-SHA2-256 keys:128, 192, 256 HMAC-SHA2-256 bits with 128, 192, HMAC-SHA2-256 bits with 128, 192, HMAC-SHA2-256 bits with 128, 192, 256 HMAC-SHA2-256 bits with 128, 192, 256 HMAC-SHA2-256 bits with 128, 192, 256 HMAC-SHA2-256 bits with 128, 192, 4MAC-SHA2-256 bits with 128, 192, 256 HMAC-SHA2-256 bits with 128, 192, 256 HMAC-SHA2-256 bits with 128, 192, 4MAC-SHA2-256 bits with 128, 192, 4MAC-SHA2-384 HMAC-SHA3-324 HMAC-SHA2-384 bits of strength HMAC-SHA2-384 bits of strength HMAC-SHA2-384 bits of strength HMAC-SHA2-384 bits with 112-256 HMAC-SHA2-312 bits with 112-256 HMAC-SHA2-512 bits with 112-256 HMAC-SHA2-512				keys:112-524288	HMAC-SHA2-224
bits of strength HMAC-SHA2-224 HMAC-SHA2-384 HMAC-SHA2-224 keys:112-524288 HMAC-SHA2-224 bits with 112-256 HMAC-SHA2-224 bits of strength HMAC-SHA2-224 HMAC-SHA2-512 HMAC-SHA2-224 HMAC-SHA2-512 HMAC-SHA2-226 bits with 112-256 HMAC-SHA2-256 bits of strength HMAC-SHA2-256 bits of strength HMAC-SHA2-256 keys:128, 192, 256 HMAC-SHA2-256 bits of strength HMAC-SHA2-256 keys:128, 192, 256 HMAC-SHA2-256 keys:128, 192, 256 HMAC-SHA2-256 bits of strength HMAC-SHA2-256 bits of strength HMAC-SHA2-256 bits of strength HMAC-SHA2-384 bits of strength HMAC-SHA2-384 <				bits with 112-256	HMAC-SHA2-224
HMAC-SHA2-384 HMAC-SHA2-224 keys:112-524288 HMAC-SHA2-224 bits with 112-256 HMAC-SHA2-224 bits of strength HMAC-SHA2-224 HMAC-SHA2-512 HMAC-SHA2-224 HMAC-SHA2-512 HMAC-SHA2-224 keys:112-524288 HMAC-SHA2-226 bits with 112-256 HMAC-SHA2-2266 bits of strength HMAC-SHA2-256 AES-CMAC HMAC-SHA2-256 keys:128, 192, 256 HMAC-SHA2-256 AES-CMAC HMAC-SHA2-256 keys:128, 192, 256 HMAC-SHA2-256 AES-GMAC HMAC-SHA2-256 keys:128, 192, 256 HMAC-SHA2-256 keys:128, 192, 256 HMAC-SHA2-256 keys:128, 192, 256 HMAC-SHA2-256 bits with 128, 192, HMAC-SHA2-256 keys:112-524288 HMAC-SHA2-384 HMAC-SHA3-224 HMAC-SHA2-384 bits of strength HMAC-S				bits of strength	HMAC-SHA2-224
keys:112-524288 HMAC-SHA2-224 bits with 112-256 HMAC-SHA2-224 bits of strength HMAC-SHA2-224 HMAC-SHA2-512 HMAC-SHA2-224 HMAC-SHA2-512 HMAC-SHA2-226 bits of strength HMAC-SHA2-256 bits with 112-256 HMAC-SHA2-256 bits of strength HMAC-SHA2-256 bits with 128, 192, 256 HMAC-SHA2-256 keys:128, 192, 256 HMAC-SHA2-256 bits with 128, 192, HMAC-SHA2-256 keys:128, 192, 256 HMAC-SHA2-256 keys:128, 192, 256 HMAC-SHA2-256 keys:128, 192, 256 HMAC-SHA2-256 bits with 128, 192, HMAC-SHA2-256 bits with 128, 192, HMAC-SHA2-256 bits with 112,54 HMAC-SHA2-256 bits with 112,54 HMAC-SHA2-384 HMAC-SHA3-324 HMAC-SHA2-384 bits of strength HMAC-SHA2-384 bits of strength HMAC-SHA2-384 bits with 112-256 HMAC-SHA2-384 bits of strength HMAC-SHA2-384 bits with 112-256 HMAC-SHA2-384 bits with 112-256 HMAC-SHA2-384				HMAC-SHA2-384	HMAC-SHA2-224
bits with 112-256 HMAC-SHA2-224 bits of strength HMAC-SHA2-224 HMAC-SHA2-512 HMAC-SHA2-226 bits with 112-256 HMAC-SHA2-256 bits of strength HMAC-SHA2-256 bits of strength HMAC-SHA2-256 bits with 128, 192, 256 HMAC-SHA2-256 bits with 128, 192, HMAC-SHA2-384 HMAC-SHA3-224 HMAC-SHA2-384 bits with 112-526 HMAC-SHA2-384 bits of strength HMAC-SHA2-384 bits with 112-256 HMAC-SHA2-384 bits with 112-256 HMAC-SHA2-384 bits of strength HMAC-SHA2-312 bits of strength HMAC-SHA2-512 HMAC-SHA3-384 HMAC-SHA2-512 bits of strength HMAC-SHA2-512 bits of strength HMAC-SHA2-512				keys:112-524288	HMAC-SHA2-224
bits of strength HMAC-SHA2-224 HMAC-SHA2-512 HMAC-SHA2-226 bits with 112-256 HMAC-SHA2-256 bits of strength HMAC-SHA2-256 bits of strength HMAC-SHA2-256 bits with 128, 192, 256 HMAC-SHA2-256 bits with 128, 192, HMAC-SHA2-384 HMAC-SHA3-224 HMAC-SHA2-384 bits with 112-256 HMAC-SHA2-384 bits with 112-256 HMAC-SHA2-384 bits with 112-256 HMAC-SHA2-384 HMAC-SHA3-328 HMAC-SHA2-384 HMAC-SHA3-384 HMAC-SHA2-384 bits with 112-256 HMAC-SHA2-512 bits with 112-256 HMAC-SHA2-512 bits with 112-256 HMAC-SHA2-512 bits with 112-256 HMAC-SHA2-512 bits with 112-256 HMAC-SHA2-512				bits with 112-256	HMAC-SHA2-224
HMAC-SHA2-512 HMAC-SHA2-224 keys:112-524288 HMAC-SHA2-256 bits with 112-256 HMAC-SHA2-256 bits of strength HMAC-SHA2-256 AES-CMAC HMAC-SHA2-256 keys:128, 192, 256 HMAC-SHA2-256 bits with 128, 192, HMAC-SHA2-256 256 bits of strength HMAC-SHA2-256 AES-GMAC HMAC-SHA2-256 bits with 128, 192, HMAC-SHA2-256 bits of strength HMAC-SHA2-384 HMAC-SHA3-224 HMAC-SHA2-384 keys:112-524288 HMAC-SHA2-384 bits of strength HMAC-SHA2-384 HMAC-SHA3-256 HMAC-SHA2-384 HMAC-SHA3-256 HMAC-SHA2-384 bits with 112-256 HMAC-SHA2-512 bits of strength HMAC-SHA2-512 bits of strength HMAC-SHA2-512 bits of strength HMAC-SHA2-512 bits with 112-25				bits of strength	HMAC-SHA2-224
keys:112-524288 HMAC-SHA2-256 bits with 112-256 HMAC-SHA2-256 bits of strength HMAC-SHA2-256 AES-CMAC HMAC-SHA2-256 keys:128, 192, 256 HMAC-SHA2-256 bits with 128, 192, HMAC-SHA2-256 256 bits of strength HMAC-SHA2-256 AES-GMAC HMAC-SHA2-256 keys:128, 192, 256 HMAC-SHA2-256 bits with 128, 192, HMAC-SHA2-256 keys:128, 192, 256 HMAC-SHA2-256 bits with 128, 192, HMAC-SHA2-256 bits with 128, 192, HMAC-SHA2-384 HMAC-SHA3-224 HMAC-SHA2-384 bits of strength HMAC-SHA2-384 bits of stre				HMAC-SHA2-512	HMAC-SHA2-224
bits with 112-256 HMAC-SHA2-256 bits of strength HMAC-SHA2-256 keys:128, 192, 256 HMAC-SHA2-256 bits with 128, 192, HMAC-SHA2-256 bits with 128, 192, HMAC-SHA2-256 AES-GMAC HMAC-SHA2-256 keys:128, 192, 256 HMAC-SHA2-256 bits with 128, 192, HMAC-SHA2-256 bits with 128, 192, HMAC-SHA2-256 bits with 128, 192, HMAC-SHA2-384 HMAC-SHA3-224 HMAC-SHA2-384 HMAC-SHA3-224 HMAC-SHA2-384 bits of strength HMAC-SHA2-384 bits of strength HMAC-SHA2-384 bits of strength HMAC-SHA2-384 bits of strength HMAC-SHA2-384 bits with 112-256 HMAC-SHA2-512 bits with 112-256 HMAC-SHA2-512 bits with 112-256 HMAC-SHA2-512 bits with 112-256 HMAC-SHA2-512				keys:112-524288	HMAC-SHA2-256
bits of strength HMAC-SHA2-256 AES-CMAC HMAC-SHA2-256 keys:128, 192, 256 HMAC-SHA2-256 bits with 128, 192, HMAC-SHA2-256 256 bits of strength HMAC-SHA2-256 AES-GMAC HMAC-SHA2-256 keys:128, 192, 256 HMAC-SHA2-256 bits with 128, 192, HMAC-SHA2-256 keys:128, 192, 256 HMAC-SHA2-256 bits with 128, 192, HMAC-SHA2-256 256 bits of strength HMAC-SHA2-256 bits with 128, 192, HMAC-SHA2-256 bits with 128, 192, HMAC-SHA2-256 bits with 128, 192, HMAC-SHA2-384 HMAC-SHA3-224 HMAC-SHA2-384 bits with 112-256 HMAC-SHA2-384 bits of strength HMAC-SHA2-512 HMAC-SHA3-384 HMAC-SHA2-512 bits with 112-256 HMAC-SHA2-512 bit				bits with 112-256	HMAC-SHA2-256
AES-CMAC HMAC-SHA2-256 keys:128, 192, 256 HMAC-SHA2-256 bits with 128, 192, HMAC-SHA2-256 256 bits of strength HMAC-SHA2-256 AES-GMAC HMAC-SHA2-256 bits with 128, 192, HMAC-SHA2-256 bits with 12-524288 HMAC-SHA2-384 bits of strength HMAC-SHA2-384 bits of strength HMAC-SHA2-384 bits with 112-256 HMAC-SHA2-384 bits of strength HMAC-SHA2-384 bits of strength HMAC-SHA2-512 HMAC-SHA3-384 HMAC-SHA2-512 bits with 112-256 HMAC-SHA2-512				bits of strength	HMAC-SHA2-256
keys:128, 192, 256 HMAC-SHA2-256 bits with 128, 192, HMAC-SHA2-256 256 bits of strength HMAC-SHA2-256 AES-GMAC HMAC-SHA2-256 keys:128, 192, 256 HMAC-SHA2-256 bits with 128, 192, HMAC-SHA2-384 HMAC-SHA3-224 HMAC-SHA2-384 bits of strength HMAC-SHA2-512 bits of strength HMAC-SHA2-512 bits with 112-256 HMAC-SHA2-512 bits of strength HMAC-SHA2-512				AES-CMAC	HMAC-SHA2-256
bits with 128, 192, HMAC-SHA2-256 256 bits of strength HMAC-SHA2-256 AES-GMAC HMAC-SHA2-256 keys:128, 192, 256 HMAC-SHA2-256 bits with 128, 192, HMAC-SHA2-256 bits with 112-256 HMAC-SHA2-384 bits of strength HMAC-SHA2-384 bits of strength HMAC-SHA2-384 bits with 112-256 HMAC-SHA2-384 bits with 112-256 HMAC-SHA2-384 bits of strength HMAC-SHA2-384 bits of strength HMAC-SHA2-384 bits of strength HMAC-SHA2-384 bits of strength HMAC-SHA2-512 bits with 112-256 HMAC-SHA2-512 <t< td=""><td></td><td></td><td></td><td>keys:128, 192, 256</td><td>HMAC-SHA2-256</td></t<>				keys:128, 192, 256	HMAC-SHA2-256
256 bits of strength HMAC-SHA2-256 AES-GMAC HMAC-SHA2-256 keys:128, 192, 256 HMAC-SHA2-256 bits with 128, 192, HMAC-SHA2-256 256 bits of strength HMAC-SHA2-384 HMAC-SHA3-224 HMAC-SHA2-384 keys:112-524288 HMAC-SHA2-384 bits with 112-256 HMAC-SHA2-384 bits of strength HMAC-SHA2-384 HMAC-SHA3-256 HMAC-SHA2-384 keys:112-524288 HMAC-SHA2-384 bits with 112-256 HMAC-SHA2-384 bits with 112-256 HMAC-SHA2-384 bits of strength HMAC-SHA2-384 bits of strength HMAC-SHA2-384 bits of strength HMAC-SHA2-384 bits with 112-256 HMAC-SHA2-384 bits of strength HMAC-SHA2-512 HMAC-SHA3-384 HMAC-SHA2-512 bits with 112-256 HMAC-SHA2-512 bits with 112-256 HMAC-SHA2-512 bits with 112-256 HMAC-SHA2-512				DITS WITH 128, 192,	HMAC-SHA2-256
AES-GMAC HMAC-SHA2-236 keys:128, 192, 256 HMAC-SHA2-256 bits with 128, 192, HMAC-SHA2-256 256 bits of strength HMAC-SHA2-384 HMAC-SHA3-224 HMAC-SHA2-384 HMAC-SHA3-224 HMAC-SHA2-384 keys:112-524288 HMAC-SHA2-384 bits with 112-256 HMAC-SHA2-384 bits of strength HMAC-SHA2-384 bits with 112-256 HMAC-SHA2-384 bits of strength HMAC-SHA2-384 bits of strength HMAC-SHA2-384 bits of strength HMAC-SHA2-384 bits of strength HMAC-SHA2-512 HMAC-SHA3-384 HMAC-SHA2-512 bits with 112-256 HMAC-SHA2-512 bits with 112-256 HMAC-SHA2-512 bits of strength HMAC-SHA2-512 bits of strength HMAC-SHA2-512				256 DIts of strength	HMAC-SHAZ-256
keys:128, 192, 256 HMAC-SHA2-256 bits with 128, 192, HMAC-SHA2-256 256 bits of strength HMAC-SHA2-384 HMAC-SHA3-224 HMAC-SHA2-384 HMAC-SHA3-224 HMAC-SHA2-384 bits with 112-524288 HMAC-SHA2-384 bits with 112-256 HMAC-SHA2-384 bits of strength HMAC-SHA2-384 bits of strength HMAC-SHA2-384 bits of strength HMAC-SHA2-384 bits of strength HMAC-SHA2-384 bits with 112-256 HMAC-SHA2-384 bits of strength HMAC-SHA2-384 bits of strength HMAC-SHA2-384 bits with 112-256 HMAC-SHA2-384 bits of strength HMAC-SHA2-512 HMAC-SHA3-384 HMAC-SHA2-512 bits with 112-256 HMAC-SHA2-512 bits with 112-256 HMAC-SHA2-512 bits with 112-256 HMAC-SHA2-512 bits with 112-256 HMAC-SHA2-512 bits of strength HMAC-SHA2-512 bits of strength HMAC-SHA2-512				AES-GMAC	
bits with 128, 192, HMAC-SHA2-230 256 bits of strength HMAC-SHA2-384 HMAC-SHA3-224 HMAC-SHA2-384 keys:112-524288 HMAC-SHA2-384 bits with 112-256 HMAC-SHA2-384 HMAC-SHA3-256 HMAC-SHA2-384 keys:112-524288 HMAC-SHA2-384 bits with 112-256 HMAC-SHA2-384 bits of strength HMAC-SHA2-384 bits of strength HMAC-SHA2-384 bits of strength HMAC-SHA2-312 HMAC-SHA3-384 HMAC-SHA2-512 keys:112-524288 HMAC-SHA2-512 bits with 112-256 HMAC-SHA2-512				Keys: 128, 192, 250	
HMAC-SHA2-384 HMAC-SHA3-224 HMAC-SHA2-384 keys:112-524288 HMAC-SHA2-384 bits with 112-256 HMAC-SHA2-384 HMAC-SHA2-384 HMAC-SHA3-256 HMAC-SHA2-384 bits with 112-256 HMAC-SHA2-384 bits of strength HMAC-SHA2-384 HMAC-SHA2-384 HMAC-SHA2-312 HMAC-SHA3-384 HMAC-SHA2-512 HMAC-SHA3-384 HMAC-SHA2-512 bits with 112-256 HMAC-SHA2-512 bits with 112-256 HMAC-SHA2-512 bits with 112-256 HMAC-SHA2-512 bits with 112-256 HMAC-SHA2-512 bits with 112-256 HMAC-SHA2-512 bits with 112-256 HMAC-SHA2-512				256 bits of strongth	
HMAC-SHA3-224 keys:112-524288 HMAC-SHA2-384 bits with 112-256 HMAC-SHA2-384 bits of strength HMAC-SHA2-384 HMAC-SHA2-384 HMAC-SHA2-384 keys:112-524288 HMAC-SHA2-384 bits with 112-256 HMAC-SHA2-384 bits of strength HMAC-SHA2-512 HMAC-SHA3-384 HMAC-SHA2-512 keys:112-524288 HMAC-SHA2-512 bits with 112-256 HMAC-SHA2-512 bits with 112-256 HMAC-SHA2-512					
bits with 112-256 HMAC-SHA2-384 bits of strength HMAC-SHA2-384 HMAC-SHA3-256 HMAC-SHA2-384 HMAC-SHA3-256 HMAC-SHA2-384 bits with 112-256 HMAC-SHA2-384 bits of strength HMAC-SHA2-512 HMAC-SHA3-384 HMAC-SHA2-512 keys:112-524288 HMAC-SHA2-512 bits with 112-256 HMAC-SHA2-512 bits with 112-256 HMAC-SHA2-512 bits of strength HMAC-SHA2-512				HMAC-SHA3-224	
bits with 112-236 HMAC-SHA2-384 bits of strength HMAC-SHA2-384 HMAC-SHA3-256 HMAC-SHA2-384 keys:112-524288 HMAC-SHA2-384 bits with 112-256 HMAC-SHA2-384 bits of strength HMAC-SHA2-512 HMAC-SHA3-384 HMAC-SHA2-512 keys:112-524288 HMAC-SHA2-512 bits with 112-256 HMAC-SHA2-512 bits of strength HMAC-SHA2-512				keys.112-524200	
HMAC-SHA2-384 HMAC-SHA3-256 HMAC-SHA2-384 keys:112-524288 HMAC-SHA2-384 bits with 112-256 HMAC-SHA2-384 bits of strength HMAC-SHA2-512 HMAC-SHA3-384 HMAC-SHA2-512 keys:112-524288 HMAC-SHA2-512 bits with 112-256 HMAC-SHA2-512 bits of strength HMAC-SHA2-512				DILS WILL I 12-250	
https://www.sinac-snac-solutions/ keys:112-524288 HMAC-SHA2-384 bits with 112-256 HMAC-SHA2-384 bits of strength HMAC-SHA2-512 HMAC-SHA3-384 HMAC-SHA2-512 keys:112-524288 HMAC-SHA2-512 bits with 112-256 HMAC-SHA2-512 bits of strength HMAC-SHA2-512				DILS OF SCIENGLIN	
bits with 112-256 HMAC-SHA2-384 bits of strength HMAC-SHA2-312 HMAC-SHA3-384 HMAC-SHA2-512 keys:112-524288 HMAC-SHA2-512 bits with 112-256 HMAC-SHA2-512 bits of strength HMAC-SHA2-512				HMAC-SHAS-230	
bits with 112-256 HMAC-SHA2-384 bits of strength HMAC-SHA2-512 HMAC-SHA3-384 HMAC-SHA2-512 keys:112-524288 HMAC-SHA2-512 bits with 112-256 HMAC-SHA2-512 bits of strength HMAC-SHA2-512				keys.112-524200	
HMAC-SHA2-S12 HMAC-SHA3-384 HMAC-SHA2-512 keys:112-524288 HMAC-SHA2-512 bits with 112-256 HMAC-SHA2-512 bits of strength HMAC-SHA2-512				bits of strep ath	
keys:112-524288 HMAC-SHA2-512 bits with 112-256 HMAC-SHA2-512 bits of strength HMAC-SHA2-512					
bits of strength HMAC-SHA2-512 HMAC-SHA2-512				1101AC-30A3-304	
bits of strength HMAC-SHA2-512				hite with 112 264	
				hits of strength	HMAC-SHA2-512
					ΗΜΔ(-SHΔ2-512

Name	Туре	Description	Properties	Algorithms
			keys:112-524288	HMAC-SHA2-512
			bits with 112-256	HMAC-SHA2-512
			bits of strength	AES-CMAC
				AES-GMAC
				HMAC-SHA3-224
				HMAC-SHA3-224
				HMAC-SHA3-256
				HMAC-SHA3-256
				HMAC-SHA3-384
				HMAC-SHA3-384
				HMAC-SHA3-512
				HMAC-SHA3-512
				SHA-1
				SHA2-224
				SHAZ-224 SHA2-224
				SHA2-224
				SHA2-256
				SHA2-384

Name	Туре	Description	Properties	Algorithms
				SHA2-384
				SHA2-512
				SHA3-224
				SHA3-224
				SHA3-256
				SHA3-256
				SHA3-384
				SHA3-256
				SHA3-512
				SHA3-512
Shared Secret	KAS-SSC	SP 800-56Ar3. KAS-	KAS-FFC-SSC	KAS-FFC-SSC
Computation with		ECC-SSC and KAS-	Sp800-56Ar3	Sp800-56Ar3
KAS-FFC-SSC or		FFC-SSC per IG D.F	keys:ffdhe2048,	KAS-ECC-SSC
KAS-ECC-SSC		Scenario 2 (1)	ffdhe3072,	Sp800-56Ar3
			ffdhe4096,	•
			ffdhe6144,	
			ffdhe8192 with	
			112-200 bits of	
			strength	
			KAS-ECC-SSC	
			Sp800-56Ar3	
			curves:P-256. P-384	
			with 128, 192 bits	
			of strength	
Message Digest	SHA	FIPS180-4, FIPS202,	SHA-1:N/A	SHA-1
with SHA		Message digest	SHA2-224:N/A	SHA-1
		······································	SHA2-256:N/A	SHA-1
			SHA2-384:N/A	SHA-1
			SHA2-512:N/A	SHA-1
			SHA3-224:N/A	SHA-1
			SHA3-256:N/A	SHA-1
			SHA3-384:N/A	SHA-1
			SHA3-512:N/A	SHA2-224
				SHA2-224 SHA2-224
				SHA2-224
				SUA2-224 SUA2-256
				SHAZ-230 SHA2-256
				SHA2-256

Name	Туре	Description	Properties	Algorithms
				SHA2-256
				SHA2-384
				SHA2-512
				SHA3-224
				SHA3-224
				SHA3-256
				SHA3-256
				SHA3-384
				SHA3-384
				SHA3-512
				SHA3-512
Key Pair Generation	AsymKeyPair-	FIPS186-4, SP800-	Safe Primes Key	Safe Primes Key
with ECDSA or Safe	KeyGen	56Ar3. ECDSA Key	Generation	Generation
Primes		pair generation	keys:ffdhe2048,	ECDSA KeyGen
		according to	ffdhe3072,	(FIPS186-4)
		FIPS186-4,	ffdhe4096,	
		Appendix B.4.2 per	ffdhe6144,	
		IG D.H and SP800-	ffdhe8192 with	
		133r2, section 4	112-200 bits of	
		(without XOR) 5.1,	strength	
		5.2; Sate Primes	ECDSA KeyGen	
		Key Generation	(FIPS186-4)	
		according to SP800-	curves:P-256, P-384	
		56Ar3, Section	with 128, 192 bits	
		5.6.1.1.4 per IG D.H	or strength	
		and SP800-133r2,		
		section 4 (without		
		XUR), 5.2		
Authenticated	BC-Auth	SP800-38C.	AES-CCM keys:128,	AES-CCM
Encryption and	KTS-Wrap	Authenticated	192, 256 bits with	AES-CCM
Authenticated		encryption,	128, 192, 256 bits	AES-CCM
Decryption with		Authenticated	or strength	AES-CCM
AES-CCM		decryption, KTS		AES-CCM
		(key wrapping and		AES-CCM
	1			AES-CCM

ubuntu[©]Canonical Ltd. Ubuntu 22.04 Kernel Crypto API Cryptographic Module FIPS 140-3 Non-Proprietary Security Policy

Name	Туре	Description	Properties	Algorithms
		key unwrapping)		
		per IG D.G		
Authenticated	BC-Auth	SP800-38D.	AES-GCM kevs:128.	AES-GCM
Decryption with	KTS-Wrap	Authenticated	192. 256 bits with	AES-GCM
AES-GCM		decryption. KTS	128, 192, 256 bits	AES-GCM
		(key unwrapping)	of strength	AES-GCM
		per IG D.G	Compliance: FIPS	AES-GCM
			140-3 IG D.G	AES-GCM
				AFS-GCM
Signature	DiaSia-SiaVer	FIPS186-4	RSA SigVer	RSA SigVer
Verification with		Signature	(FIDS186-4)	(FIDS186-4)
		verification	kevs:4096 hits with	RSA SigVer
NJA .		verification	150 hits of strength	(FIDS186-4)
			150 bits of scienger	
				(FIDS186-4)
				RSA SigVer
				(FIPS186-4)
				RSA SigVer
				(FIDS186-4)
				(Π 5100 4) SHΔ-1
				SHΔ2-224
				SHA2-256
				SHA2-384
				SHA2-512
				SHA-1
				SHA2-224
				SHA2-256
				SHA2-384
				SHA2-512
				SHA-1
				SHA 7-224
				SHA2-256
				SHA2-384
				SHΔ2-512
				SHA-1
				SHA2-224
				SHΔ2-256
				SHA2-230
				SUA2-304 SUA2-512
				SHΔ2-224
				SHA2-224

ubuntu⁹Canonical Ltd. Ubuntu 22.04 Kernel Crypto API Cryptographic Module FIPS 140-3 Non-Proprietary Security Policy

Name	Туре	Description	Properties	Algorithms
				SHA2-256
				SHA2-384
				SHA2-512
Authenticated	BC-Auth	SP800-38D.	AES-GCM kevs:128.	AES-GCM
Encryption with	KTS-Wrap	Authenticated	192, 256 bits with	AES-GCM
AES-GCM		encryption KTS (key	128, 192, 256 bits	AES-GCM
		wrapping) per IG	of strength	AFS-GCM
			or screngen	AFS-GCM
		0.0		AES-GCM
				AES-GCM
				AES-CCM
				ALS-OCM
				ALS-OCM
				AES-GCM
Authenticated	BC-Auth	SP800-38A, FIPS	AES-CBC keys:128,	HMAC-SHA-1
Encryption and	KTS-Wrap	198-1. KTS (key	192, 256 bits with	HMAC-SHA2-256
Authenticated		wrapping and key	128, 192, 256 bits	HMAC-SHA2-384
Decryption with		unwrapping) per IG	of security	HMAC-SHA2-512
AES-CBC or AES-		D.G	AES-CTR keys:128,	HMAC-SHA-1
CTR with HMAC			192, 256 bits with	HMAC-SHA2-256
			128, 192, 256 bits	HMAC-SHA2-384
			of security	HMAC-SHA2-512
			HMAC-SHA-1	HMAC-SHA-1
			keys:112-524288	HMAC-SHA2-256
			bits with 112-256	HMAC-SHA2-384
			bits of security	HMAC-SHA2-512
			HMAC-SHA2-256	HMAC-SHA-1
			kevs:112-524288	HMAC-SHA2-256
			bits with 112-256	HMAC-SHA2-384
			bits of security	HMAC-SHA2-512
			HMAC-SHA2-384	HMAC-SHA-1
			kevs:112-524288	HMAC-SHA2-256
			bits with 112-256	HMAC-SHA2-384
			hits of security	ΗΜΔC-SHΔ2-512
			ΗΜΑC-SHΔ2-512	ΗΜΑζ-SHΔ-1
			kevs:112-524288	ΗΜΑC-SHΔ2-256
			hits with 112-256	ΗΜΔC-SHΔ2-384
			hits of security	ΗΜΔ(-SHΔ2-512
			Sits of security	ΗΜΔC-SHΔ-1
				111VIAC-30742-230
				ПМАС-ЭПА2-384 ЦМАС СЦАЭ 51Э
	1	1	1	HMAC-SHA2-256

Name	Туре	Description	Properties	Algorithms
				HMAC-SHA2-256
				HMAC-SHA2-384
				HMAC-SHA2-512
				AES-CBC
				AES-CTR
				SHA-1
				SHA2-256
				SHA2-250
				2002-200
				5HA2-230 SHA2-384
				SHA2-304 SHA2-384
				SHA2-384
				SHA2-512

Table 8: Security Function Implementations

2.7 Algorithm Specific Information

2.7.1 AES GCM IV

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

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

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

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

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

2.7.2 AES XTS

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

The XTS mode shall only be used for the cryptographic protection of data on storage devices. It shall not be used for other purposes, such as the encryption of data in transit. To meet the requirement stated in IG C.I, the module implements a check to ensure that the two AES keys used in AES XTS mode are not identical.

2.7.3 Diffie-Hellman and EC Diffie-Hellman

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

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

- 2. As part of the module's shared secret computation service, the module internally performs the public key validation on the peer's public key passed in as input to the API function. This meets the public key validity assurance required by the sections 5.6.2.2.1/5.6.2.2.2 of SP 800-56Ar3.
- 3. The module does not support static keys, therefore the "assurance of peer's possession of private key" is not applicable.

2.7.4 SHA-3

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

2.7.5 RSA

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

2.8 RBG and Entropy

	Cert	Vendor				
	Number	Name				
	E59	Canonical Ltd.				
Table 9: Entropy Certificates						

Name **Operational Environment** Sample Entropy Conditioning Туре Component Size рег Sample Ubuntu 22.04 LTS 64-bit on Intel(R) Xeon(R) Canonical Non-64 bits 59.43 Linear-Kernel CPU Physical Gold 6226 on Supermicro SYS-1019P-WTR; bits Feedback Shift Ubuntu Core 22 64-bit on Intel(R) Xeon(R) Register (LFSR) Time Jitter **RNG Entropy** Gold 6226 on Supermicro SYS-1019P-WTR; Ubuntu 22.04 LTS 64-bit on AWS Graviton2 source on Amazon Web Services (AWS) c6g.metal; Ubuntu Core 22 64-bit on AWS Graviton2 on Amazon Web Services (AWS) c6g.metal; Ubuntu 22.04 LTS 64-bit on IBM z15 on IBM z15

Table 10: Entropy Sources

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

Additionally, the module employs a specific HMAC SHA-512 DRBG implementation for internal purposes (e.g. to generate asymmetric key pairs). This DRBG is initially seeded with

448 output bits from the entropy source (416 bits of entropy) and reseeded with 320 output bits from the entropy source (297 bits of entropy).

2.9 Key Generation

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

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

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

2.10 Key Establishment

The module implements SSP agreement and SSP transport methods as listed in the *Security Function Implementations* table. The module implements the following SSP establishment methods:

Key agreement:

- KAS-FFC-SSC compliant with SP 800-56Ar3 and Scenario 2 (1) of FIPS 140-3 IG D.F; using ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192 safe primes groups with 112-200 bits of security strength.
- KAS-ECC-SSC compliant with SP 800-56Ar3 and Scenario 2 (1) of FIPS 140-3 IG D.F; using P-256, P-384 curves with 128, 192 bits of security strength.

Key transport:

- AES-KW according to IG D.G, using 128, 192, 256-bit keys with 128-256 bits of security strength.
- AES-CCM according to IG D.G, using 128, 192, 256-bit keys with 128-256 bits of security strength.
- AES-GCM according to IG D.G, using 128, 192, 256-bit keys with 128-256 bits of security strength.
- AES-CBC or AES-CTR with HMAC SHA-1, HMAC SHA-256, HMAC SHA-384, or HMAC SHA-512 according to IG D.G, using 128, 192, 256-bit AES keys with 128-256 bits of

security strength, and 112-524288 bits HMAC keys with 112-256 bits of security strength.

2.11 Industry Protocols

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

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

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

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

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

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

Table 11: Ports and Interfaces

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

4 Roles, Services, and Authentication

4.1 Authentication Methods

N/A for this module.

4.2 Roles

Name	Туре	Operator Type	Authentication Methods
СО	Role	СО	None
	Table	12: Roles	

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

4.3 Approved Services

Name	Descriptio n	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	со
Encryption	Encrypt a plaintext	crypto_skcipher_setkey returns 0	AES Key, plaintext	Ciphertex t	Encryption and Decryption with AES	CO - AES Key: W,E
Decryption	Decrypt a ciphertext	crypto_skcipher_setkey returns 0	AES Key, cipherte xt	Plaintext	Encryption and Decryption with AES	CO - AES Key: W,E
Authenticat ed Encryption	Encrypt a plaintext	For all except AES GCM: crypto_aead_setkey returns 0; For AES GCM: crypto_aead_get_flags(tfm) has the CRYPTO_ALG_FIPS140_COMP LIANT flag set	AES Key, IV, plaintext	Ciphertex t, MAC tag	Authenticat ed Encryption and Authenticat ed Decryption with AES- CCM Authenticat ed Encryption with AES- GCM Authenticat ed Encryption and Authenticat ed	CO - AES Key: W,E

© 2024 Canonical Ltd. / atsec information security.

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

Name	Descriptio	Indicator	Inputs	Outputs	Security	SSP
					Decryption with AES- CBC or AES- CTR with HMAC	Access
Authenticat ed 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_COMP LIANT flag set	AES key, IV, MAC tag, cipherte xt	Plaintext or failure	Authenticat ed Encryption and Authenticat ed Decryption with AES- CCM Authenticat ed Decryption with AES- GCM Authenticat ed Encryption and Authenticat ed Decryption with AES- CBC or AES- CTR with HMAC	CO - AES Key: W,E
Message Authenticati on	Compute a MAC tag	crypto_shash_init returns 0	AES Key or HMAC key, message	MAC tag	Message Authenticati on with AES or HMAC	CO - AES Key: W,E - HMAC Key: W,E
Random Number Generation	Generate random bytes	crypto_rng_get_bytes returns 0	Output length	Random bytes	Random Number Generation with HMAC DRBG, Hash DRBG or Counter DRBG	CO - Entropy Input (IG D.L): W,E - DRBG Seed (IG D.L): G,E - DRBG Internal State (V, Key) (IG D.L): G,W,E - DRBG Internal State (V, C) (IG D.L): G W F

ubuntu[©]Canonical Ltd. Ubuntu 22.04 Kernel Crypto API Cryptographic Module FIPS 140-3 Non-Proprietary Security Policy

Name	Descriptio	Indicator	Inputs	Outputs	Security	SSP
Shared Secret Computatio n	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 Computatio n 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; ECDSA: Curve	Safe Primes: DH private key, DH public key; ECDSA: EC private key, EC public key	Key Pair Generation with ECDSA or Safe Primes	CO - Intermedia te Key Generatio n Value: G,E,Z - DH Public Key: G,R - DH Private Key: G,R - EC Public Key: G,R - EC Private Key: G,R
Error Detection Code	Compute an EDC (crc32, crct10dif)	None	Message	EDC	None	co
Compressio n	Compress data (deflate, lz4, lz4hc, lzo, zlib- deflate, zstd)	None	Data	Compress ed data	None	со
Generic System Call	Use the kernel to perform various non- cryptograp hic operations	None	Identifie r, various argumen ts	Various return values	None	СО
Show Version	Return the module name and version	None	N/A	Module name and version	None	со

ubuntu[©]Canonical Ltd. Ubuntu 22.04 Kernel Crypto API Cryptographic Module FIPS 140-3 Non-Proprietary Security Policy

Name	Descriptio	Indicator	Inputs	Outputs	Security	SSP
	n is formatio				Functions	Access
	n					
Show Status	Return the module	None	N/A	Module status	None	со
Self-Test	status 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 Authenticati on with AES or HMAC Shared Secret Computatio n with KAS- FFC-SSC or KAS-ECC- SSC Message Digest with SHA Authenticat ed Encryption and Authenticat ed Decryption with AES- CCM Authenticat ed Decryption with AES- GCM Signature Verification with RSA Authenticat ed Encryption	CO

Name	Descriptio	Indicator	Inputs	Outputs	Security Functions	SSP Access
Zeroization	n Zeroize all SSPs	None	AnySSP	N/A	Functions None	Access CO - AES Key: Z - HMAC Key: Z - Shared Secret: Z - Entropy Input (IG D.L): Z - DRBG Internal State (V, Key) (IG D.L): Z - DRBG Internal State (V, Key) (IG D.L): Z - DRBG Internal State (V, C) (IG D.L): Z - DH Public Key: Z - DH Private Key: Z - EC Private Key: Z - EC
						te Key Generatio n Value: 7

Table 13: Approved Services

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

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

4.4 Non-Approved Services

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

Table 14: Non-Approved Services

4.5 External Software/Firmware Loaded

Not applicable.
5 Software/Firmware Security

5.1 Integrity Techniques

The Linux kernel binary is integrity tested using an HMAC SHA-512 calculation performed by the sha512hmac utility (which utilizes the module's HMAC and SHA-512 implementations). The kernel crypto object files listed in the *Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets)* table are loaded on start-up by the module and verified using RSA signature verification with PKCS#1 v1.5 padding, SHA-512, and a 4096-bit key.

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

5.2 Initiate on Demand

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

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Modifiable

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

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

6.2 Configuration Settings and Restrictions

The module shall be installed as specified in Section 11.1.

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

ubuntu[©]Canonical Ltd. Ubuntu 22.04 Kernel Crypto API Cryptographic Module FIPS 140-3 Non-Proprietary Security Policy

7 Physical Security

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

8 Non-Invasive Security

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

9 Sensitive Security Parameters Management

9.1 Storage Areas

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

Table 15: Storage Areas

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

9.2 SSP Input-Output Methods

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

Table 16: SSP Input-Output Methods

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
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
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 when power is removed.	By removing power

Table 17: SSP Zeroization Methods

© 2024 Canonical Ltd. / atsec information security.

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

All data output is inhibited during zeroization.

9.4 SSPs

Name	Description	Size - Strength	Туре -	Generated	Established	Used By
			Category	Ву	Ву	
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, CMAC: 128, 192, 256 bits - XTS: 128, 256 bits; ECB, CBC, CTR, CFB128, CBC- CTS-CS3, KW, OFB, CCM, GCM, CMAC, CMAC: 128, 192, 256 bits	Symmetric key - CSP			Encryption and Decryption with AES Message Authentication with AES or HMAC
HMAC Key	HMAC key used for Message authentication code (MAC);	112-524288 bits - 112-256 bits	Symmetric key - CSP			Message Authentication with AES or 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	128-448 bits - 128-256 bits	Entropy input - CSP			Random Number Generation with HMAC DRBG, Hash DRBG or Counter DRBG
DRBG Seed (IG D.L)	DRBG seed derived from Entropy Input	Counter DRBG: 256, 320, 384 bits; Hash_DRBG: 440, 888 bits; HMAC DRBG: 160, 256, 512 bits - Counter DRBG: 128, 192,	Seed - CSP	Random Number Generation with HMAC DRBG, Hash DRBG or Counter DRBG		Random Number Generation with HMAC DRBG, Hash DRBG or Counter DRBG

Name	Description	Size - Strength	Type - Category	Generated Bv	Established By	Used By
		256 bits; Hash DRBG: 128, 256 bits; HMAC DRBG: 128, 256 bits				
DRBG Internal State (V, Key) (IG D.L)	Internal state of Counter DRBG and HMAC DRBG instances	Counter DRBG: 256, 320, 348 bits; HMAC DRBG: 320, 512, 1024 bits - Counter DRBG: 128, 192, 256 bits; HMAC DRBG: 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
DRBG Internal State (V, C) (IG D.L)	Internal state of Hash DRBG instance	440, 888 bits - 128, 256 bits	Internal state - CSP	Random Number Generation with HMAC DRBG, Hash DRBG or Counter DRBG		Random Number Generation with HMAC DRBG, Hash DRBG or Counter DRBG
DH Public Key	Public key used for KAS-FFC- SSC	ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192 - 112-200 bits	Public key - PSP	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
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

Name	Input - Output	Storage	Storage	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
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 DRBG Internal State (V, Key) (IG D.L):Derives DRBG Internal State (V, C) (IG D.L):Derives
DRBG Internal State (V, Key) (IG D.L)		RAM:Plaintext	From service invocation to service completion	Free cipher handle Remove power from the module	DRBG Seed (IG D.L):Derived From
DRBG Internal State (V, C) (IG D.L)		RAM:Plaintext	From service invocation to service completion	Free cipher handle Remove power from the module	DRBG Seed (IG D.L):Derived From
DH Public Key	API input parameters; AF_ALG_type sockets (input) API output parameters; AF_ALG type sockets (output)	RAM:Plaintext	From service invocation to service completion	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	RAM:Plaintext	From service invocation to	Free cipher handle Remove	DH Public Key:Paired With Shared

Table 18: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	sockets (input) API output parameters; AF_ALG type sockets (output)		service completion	power from the module	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

Table 19: 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, 2030.

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

10 Self-Tests

10.1 Pre-Operational Self-Tests

Algorithm or	Test	Test Method	Test	Indicator	Details
Test	Properties		Туре		
HMAC-SHA2- 256 (A3812)	128-bit key	Message Authentication	SW/FW Integrity	Module becomes operational and services are available for use	Used for libkcapi
HMAC-SHA2- 256 (A3813)	128-bit key	Message Authentication	SW/FW Integrity	Module becomes operational and services are available for use	Used for libkcapi
HMAC-SHA2- 256 (A3814)	128-bit key	Message Authentication	SW/FW Integrity	Module becomes operational and services are available for use	Used for libkcapi
HMAC-SHA2- 256 (A3832)	128-bit key	Message Authentication	SW/FW Integrity	Module becomes operational and services are available for use	Used for libkcapi
HMAC-SHA2- 256 (A3850)	128-bit key	Message Authentication	SW/FW Integrity	Module becomes operational and services are available for use	Used for libkcapi
HMAC-SHA2- 256 (A3851)	128-bit key	Message Authentication	SW/FW Integrity	Module becomes operational and services are available for use	Used for libkcapi
HMAC-SHA2- 256 (A3852)	128-bit key	Message Authentication	SW/FW Integrity	Module becomes operational and services are available for use	Used for libkcapi
HMAC-SHA2- 256 (A3853)	128-bit key	Message Authentication	SW/FW Integrity	Module becomes operational and services are available for use	Used for libkcapi
HMAC-SHA2- 256 (A3857)	128-bit key	Message Authentication	SW/FW Integrity	Module becomes operational and services are available for use	Used for libkcapi
HMAC-SHA2- 256 (A3858)	128-bit key	Message Authentication	SW/FW Integrity	Module becomes operational and services are available for use	Used for libkcapi
HMAC-SHA2- 512 (A3812)	128-bit key	Message Authentication	SW/FW Integrity	Module becomes operational and services are available for use	Used for kernel and sha512hmac binaries
HMAC-SHA2- 512 (A3813)	128-bit key	Message Authentication	SW/FW Integrity	Module becomes operational and	Used for kernel and sha512hmac binaries

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
				services are available for use	
HMAC-SHA2- 512 (A3814)	128-bit key	Message Authentication	SW/FW Integrity	Module becomes operational and services are available for use	Used for kernel and sha512hmac binaries
HMAC-SHA2- 512 (A3832)	128-bit key	Message Authentication	SW/FW Integrity	Module becomes operational and services are available for use	Used for kernel and sha512hmac binaries
HMAC-SHA2- 512 (A3850)	128-bit key	Message Authentication	SW/FW Integrity	Module becomes operational and services are available for use	Used for kernel and sha512hmac binaries
HMAC-SHA2- 512 (A3851)	128-bit key	Message Authentication	SW/FW Integrity	Module becomes operational and services are available for use	Used for kernel and sha512hmac binaries
HMAC-SHA2- 512 (A3852)	128-bit key	Message Authentication	SW/FW Integrity	Module becomes operational and services are available for use	Used for kernel and sha512hmac binaries
HMAC-SHA2- 512 (A3858)	128-bit key	Message Authentication	SW/FW Integrity	Module becomes operational and services are available for use	Used for kernel and sha512hmac binaries
RSA SigVer (FIPS186-4) (A3814)	4096-bit key with SHA-512	Signature Verification	SW/FW Integrity	Module becomes operational and services are available for use	Used for kernel crypto object files
RSA SigVer (FIPS186-4) (A3832)	4096-bit key with SHA-512	Signature Verification	SW/FW Integrity	Module becomes operational and services are available for use	Used for kernel crypto object files
RSA SigVer (FIPS186-4) (A3850)	4096-bit key with SHA-512	Signature Verification	SW/FW Integrity	Module becomes operational and services are available for use	Used for kernel crypto object files
RSA SigVer (FIPS186-4) (A3851)	4096-bit key with SHA-512	Signature Verification	SW/FW Integrity	Module becomes operational and services are available for use	Used for kernel crypto object files
RSA SigVer (FIPS186-4) (A3852)	4096-bit key with SHA-512	Signature Verification	SW/FW Integrity	Module becomes operational and services are available for use	Used for kernel crypto object files

Table 20: Pre-Operational Self-Tests

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

10.2 Conditional Self-Tests

Algorithm or	Test Properties	Test	Test	Indicator	Details	Conditions
Test		Method	Туре			
AES-ECB	128, 192, 256 bit	КАТ	CAST	Module	Encryption	Test runs at
(A3812)	keys, encrypt			Decomes		power-on
				operational and		intogrity tost
						integrity test
	128 102 256 bit	KVI	CAST	Modulo	Encryption	Tost sups at
(A 3813)	kevs encrypt	NA I	CASI	hecomes	спстурсюп	
(43013)	keys, energe			operational and		before the
				services are		integrity test
				available for use		integrity test
AES-ECB	128, 192, 256 bit	КАТ	CAST	Module	Encryption	Test runs at
(A3814)	keys, encrypt			becomes		power-on
	5. 51			operational and		before the
				services are		integrity test
				available for use		
AES-ECB	128, 192, 256 bit	KAT	CAST	Module	Encryption	Test runs at
(A3820)	keys, encrypt			becomes		power-on
				operational and		before the
				services are		integrity test
				available for use		
AES-ECB	128, 192, 256 bit	KAT	CAST	Module	Encryption	Test runs at
(A3821)	keys, encrypt			becomes		power-on
				operational and		Derore the
						integrity test
	120 102 256 bit	V AT	CAST	Available for use	Encouption	Tost supe at
AES-ECB (A3822)	120, 192, 230 Dic	NAT	CASI	hecomes	Епстурскоп	
(A3022)	keys, energe			operational and		before the
				services are		integrity test
				available for use		
AES-ECB	128, 192, 256 bit	KAT	CAST	Module	Encryption	Test runs at
(A3824)	keys, encrypt			becomes		power-on
				operational and		before the
				services are		integrity test
				available for use		
AES-ECB	128, 192, 256 bit	KAT	CAST	Module	Encryption	Test runs at
(A3825)	keys, encrypt			becomes		power-on
				operational and		before the
				services are		incegrity test
	120 102 256 hit		CACT	available for use	Fo contino	Test succes
AES-ECB (A 3920)	128, 192, 250 DIL	KAT	CASI	hoodule	Епстурион	
(A3629)	keys, encrypt			operational and		before the
				services are		integrity test
				available for use		
AES-ECB	128, 192, 256 bit	КАТ	CAST	Module	Encryption	Test runs at
(A3830)	keys, encrypt			becomes		power-on
				operational and		before the
				services are		integrity test
				available for use		

Algorithm or	Test Properties	Test Method	Test	Indicator	Details	Conditions
AES-ECB (A3831)	128, 192, 256 bit keys, encrypt	KAT	CAST	Module becomes	Encryption	Test runs at power-on
				operational and services are available for use		before the integrity test
AES-ECB (A3832)	128, 192, 256 bit keys, encrypt	КАТ	CAST	Module becomes	Encryption	Test runs at power-on
				services are available for use		integrity test
AES-ECB (A3833)	128, 192, 256 bit keys, encrypt	КАТ	CAST	Module becomes operational and services are available for use	Encryption	Test runs at power-on before the integrity test
AES-ECB (A3834)	128, 192, 256 bit keys, encrypt	КАТ	CAST	Module becomes operational and services are available for use	Encryption	Test runs at power-on before the integrity test
AES-ECB (A3840)	128, 192, 256 bit keys, encrypt	КАТ	CAST	Module becomes operational and services are available for use	Encryption	Test runs at power-on before the integrity test
AES-ECB (A3841)	128, 192, 256 bit keys, encrypt	КАТ	CAST	Module becomes operational and services are available for use	Encryption	Test runs at power-on before the integrity test
AES-ECB (A3842)	128, 192, 256 bit keys, encrypt	КАТ	CAST	Module becomes operational and services are available for use	Encryption	Test runs at power-on before the integrity test
AES-ECB (A3843)	128, 192, 256 bit keys, encrypt	КАТ	CAST	Module becomes operational and services are available for use	Encryption	Test runs at power-on before the integrity test
AES-ECB (A3844)	128, 192, 256 bit keys, encrypt	КАТ	CAST	Module becomes operational and services are available for use	Encryption	Test runs at power-on before the integrity test
AES-ECB (A3845)	128, 192, 256 bit keys, encrypt	КАТ	CAST	Module becomes operational and services are available for use	Encryption	Test runs at power-on before the integrity test
AES-ECB (A3853)	128, 192, 256 bit keys, encrypt	КАТ	CAST	Module becomes operational and	Encryption	Test runs at power-on

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
		in centre	Type	services are available for use		before the integrity test
AES-ECB (A3854)	128, 192, 256 bit keys, encrypt	КАТ	CAST	Module becomes operational and services are available for use	Encryption	Test runs at power-on before the integrity test
AES-ECB (A3855)	128, 192, 256 bit keys, encrypt	КАТ	CAST	Module becomes operational and services are available for use	Encryption	Test runs at power-on before the integrity test
AES-ECB (A3856)	128, 192, 256 bit keys, encrypt	KAT	CAST	Module becomes operational and services are available for use	Encryption	Test runs at power-on before the integrity test
AES-ECB (A3857)	128, 192, 256 bit keys, encrypt	КАТ	CAST	Module becomes operational and services are available for use	Encryption	Test runs at power-on before the integrity test
AES-ECB (A3812)	128, 192, 256 bit keys, decrypt	КАТ	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-ECB (A3813)	128, 192, 256 bit keys, decrypt	KAT	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-ECB (A3814)	128, 192, 256 bit keys, decrypt	КАТ	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-ECB (A3820)	128, 192, 256 bit keys, decrypt	КАТ	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-ECB (A3821)	128, 192, 256 bit keys, decrypt	KAT	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-ECB (A3822)	128, 192, 256 bit keys, decrypt	КАТ	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-ECB (A3824)	128, 192, 256 bit keys, decrypt	KAT	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-ECB (A3825)	128, 192, 256 bit keys, decrypt	КАТ	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-ECB (A3829)	128, 192, 256 bit keys, decrypt	КАТ	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-ECB (A3830)	128, 192, 256 bit keys, decrypt	КАТ	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-ECB (A3831)	128, 192, 256 bit keys, decrypt	КАТ	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-ECB (A3832)	128, 192, 256 bit keys, decrypt	KAT	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-ECB (A3833)	128, 192, 256 bit keys, decrypt	КАТ	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-ECB (A3834)	128, 192, 256 bit keys, decrypt	КАТ	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-ECB (A3840)	128, 192, 256 bit keys, decrypt	КАТ	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-ECB (A3841)	128, 192, 256 bit keys, decrypt	КАТ	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-ECB (A3842)	128, 192, 256 bit keys, decrypt	KAT	CAST	Module becomes operational and	Decryption	Test runs at power-on

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
		in centre	Type	services are available for use		before the integrity test
AES-ECB (A3843)	128, 192, 256 bit keys, decrypt	КАТ	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-ECB (A3844)	128, 192, 256 bit keys, decrypt	КАТ	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-ECB (A3845)	128, 192, 256 bit keys, decrypt	КАТ	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-ECB (A3853)	128, 192, 256 bit keys, decrypt	КАТ	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-ECB (A3854)	128, 192, 256 bit keys, decrypt	КАТ	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-ECB (A3855)	128, 192, 256 bit keys, decrypt	КАТ	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-ECB (A3856)	128, 192, 256 bit keys, decrypt	КАТ	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-ECB (A3857)	128, 192, 256 bit keys, decrypt	КАТ	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-CBC (A3814)	128, 192, 256 bit keys, encrypt	KAT	CAST	Module becomes operational and services are available for use	Encryption	Test runs at power-on before the integrity test
AES-CBC (A3822)	128, 192, 256 bit keys, encrypt	КАТ	CAST	Module becomes operational and services are available for use	Encryption	Test runs at power-on before the integrity test

Algorithm or Test	Test Properties	Test Method	Test	Indicator	Details	Conditions
AES-CBC (A3829)	128, 192, 256 bit keys, encrypt	KAT	CAST	Module becomes	Encryption	Test runs at power-on
	57 51			operational and services are available for use		before the integrity test
AES-CBC	128, 192, 256 bit	KAT	CAST	Module	Encryption	Test runs at
(A3832)	keys, encrypt			becomes operational and services are available for use		power-on before the integrity test
AES-CBC (A3840)	128, 192, 256 bit keys, encrypt	КАТ	CAST	Module becomes operational and services are available for use	Encryption	Test runs at power-on before the integrity test
AES-CBC (A3843)	128, 192, 256 bit keys, encrypt	КАТ	CAST	Module becomes operational and services are available for use	Encryption	Test runs at power-on before the integrity test
AES-CBC (A3853)	128, 192, 256 bit keys, encrypt	КАТ	CAST	Module becomes operational and services are available for use	Encryption	Test runs at power-on before the integrity test
AES-CBC (A3854)	128, 192, 256 bit keys, encrypt	КАТ	CAST	Module becomes operational and services are available for use	Encryption	Test runs at power-on before the integrity test
AES-CBC (A3857)	128, 192, 256 bit keys, encrypt	КАТ	CAST	Module becomes operational and services are available for use	Encryption	Test runs at power-on before the integrity test
AES-CBC (A3814)	128, 192, 256 bit keys, decrypt	КАТ	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-CBC (A3822)	128, 192, 256 bit keys, decrypt	КАТ	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-CBC (A3829)	128, 192, 256 bit keys, decrypt	КАТ	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-CBC (A3832)	128, 192, 256 bit keys, decrypt	КАТ	CAST	Module becomes operational and	Decryption	Test runs at power-on

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
			Type	services are available for use		before the integrity test
AES-CBC (A3840)	128, 192, 256 bit keys, decrypt	КАТ	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-CBC (A3843)	128, 192, 256 bit keys, decrypt	КАТ	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-CBC (A3853)	128, 192, 256 bit keys, decrypt	КАТ	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-CBC (A3854)	128, 192, 256 bit keys, decrypt	КАТ	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-CBC (A3857)	128, 192, 256 bit keys, decrypt	КАТ	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-CBC-CS3 (A3819)	128 bit keys, encrypt	КАТ	CAST	Module becomes operational and services are available for use	Encryption	Test runs at power-on before the integrity test
AES-CBC-CS3 (A3828)	128 bit keys, encrypt	КАТ	CAST	Module becomes operational and services are available for use	Encryption	Test runs at power-on before the integrity test
AES-CBC-CS3 (A3838)	128 bit keys, encrypt	КАТ	CAST	Module becomes operational and services are available for use	Encryption	Test runs at power-on before the integrity test
AES-CBC-CS3 (A3849)	128 bit keys, encrypt	КАТ	CAST	Module becomes operational and services are available for use	Encryption	Test runs at power-on before the integrity test
AES-CBC-CS3 (A3853)	128 bit keys, encrypt	КАТ	CAST	Module becomes operational and services are available for use	Encryption	Test runs at power-on before the integrity test

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-CBC-CS3 (A3854)	128 bit keys, encrypt	КАТ	CAST	Module becomes operational and services are available for use	Encryption	Test runs at power-on before the integrity test
AES-CBC-CS3 (A3819)	128 bit keys, decrypt	КАТ	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-CBC-CS3 (A3828)	128 bit keys, decrypt	КАТ	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-CBC-CS3 (A3838)	128 bit keys, decrypt	КАТ	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-CBC-CS3 (A3849)	128 bit keys, decrypt	КАТ	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-CBC-CS3 (A3853)	128 bit keys, decrypt	КАТ	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-CBC-CS3 (A3854)	128 bit keys, decrypt	КАТ	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-CFB128 (A3817)	128, 192, 256 bit keys, encrypt	КАТ	CAST	Module becomes operational and services are available for use	Encryption	Test runs at power-on before the integrity test
AES-CFB128 (A3826)	128, 192, 256 bit keys, encrypt	КАТ	CAST	Module becomes operational and services are available for use	Encryption	Test runs at power-on before the integrity test
AES-CFB128 (A3836)	128, 192, 256 bit keys, encrypt	КАТ	CAST	Module becomes operational and services are available for use	Encryption	Test runs at power-on before the integrity test
AES-CFB128 (A3847)	128, 192, 256 bit keys, encrypt	КАТ	CAST	Module becomes operational and	Encryption	Test runs at power-on

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
		in centre	Type	services are available for use		before the integrity test
AES-CFB128 (A3854)	128, 192, 256 bit keys, encrypt	КАТ	CAST	Module becomes operational and services are available for use	Encryption	Test runs at power-on before the integrity test
AES-CFB128 (A3817)	128, 192, 256 bit keys, decrypt	КАТ	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-CFB128 (A3826)	128, 192, 256 bit keys, decrypt	КАТ	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-CFB128 (A3836)	128, 192, 256 bit keys, decrypt	КАТ	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-CFB128 (A3847)	128, 192, 256 bit keys, decrypt	КАТ	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-CFB128 (A3854)	128, 192, 256 bit keys, decrypt	КАТ	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-CTR (A3814)	128, 192, 256 bit keys, encrypt	КАТ	CAST	Module becomes operational and services are available for use	Encryption	Test runs at power-on before the integrity test
AES-CTR (A3822)	128, 192, 256 bit keys, encrypt	КАТ	CAST	Module becomes operational and services are available for use	Encryption	Test runs at power-on before the integrity test
AES-CTR (A3829)	128, 192, 256 bit keys, encrypt	KAT	CAST	Module becomes operational and services are available for use	Encryption	Test runs at power-on before the integrity test
AES-CTR (A3832)	128, 192, 256 bit keys, encrypt	KAT	CAST	Module becomes operational and services are available for use	Encryption	Test runs at power-on before the integrity test

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-CTR (A3840)	128, 192, 256 bit keys, encrypt	КАТ	CAST	Module becomes	Encryption	Test runs at power-on
				operational and services are available for use		before the integrity test
AES-CTR (A3843)	128, 192, 256 bit keys, encrypt	КАТ	CAST	Module becomes operational and services are available for use	Encryption	Test runs at power-on before the integrity test
AES-CTR (A3853)	128, 192, 256 bit keys, encrypt	КАТ	CAST	Module becomes operational and services are available for use	Encryption	Test runs at power-on before the integrity test
AES-CTR (A3854)	128, 192, 256 bit keys, encrypt	КАТ	CAST	Module becomes operational and services are available for use	Encryption	Test runs at power-on before the integrity test
AES-CTR (A3857)	128, 192, 256 bit keys, encrypt	КАТ	CAST	Module becomes operational and services are available for use	Encryption	Test runs at power-on before the integrity test
AES-CTR (A3814)	128, 192, 256 bit keys, decrypt	КАТ	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-CTR (A3822)	128, 192, 256 bit keys, decrypt	КАТ	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-CTR (A3829)	128, 192, 256 bit keys, decrypt	КАТ	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-CTR (A3832)	128, 192, 256 bit keys, decrypt	КАТ	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-CTR (A3840)	128, 192, 256 bit keys, decrypt	КАТ	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-CTR (A3843)	128, 192, 256 bit keys, decrypt	КАТ	CAST	Module becomes operational and	Decryption	Test runs at power-on

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				services are available for use		before the integrity test
AES-CTR (A3853)	128, 192, 256 bit keys, decrypt	КАТ	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-CTR (A3854)	128, 192, 256 bit keys, decrypt	КАТ	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-CTR (A3857)	128, 192, 256 bit keys, decrypt	КАТ	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-CCM (A3814)	128, 192, 256 bit keys, 128-bit IVs, encrypt	КАТ	CAST	Module becomes operational and services are available for use	Encryption	Test runs at power-on before the integrity test
AES-CCM (A3822)	128, 192, 256 bit keys, 128-bit IVs, encrypt	КАТ	CAST	Module becomes operational and services are available for use	Encryption	Test runs at power-on before the integrity test
AES-CCM (A3829)	128, 192, 256 bit keys, 128-bit IVs, encrypt	KAT	CAST	Module becomes operational and services are available for use	Encryption	Test runs at power-on before the integrity test
AES-CCM (A3832)	128, 192, 256 bit keys, 128-bit IVs, encrypt	КАТ	CAST	Module becomes operational and services are available for use	Encryption	Test runs at power-on before the integrity test
AES-CCM (A3843)	128, 192, 256 bit keys, 128-bit IVs, encrypt	КАТ	CAST	Module becomes operational and services are available for use	Encryption	Test runs at power-on before the integrity test
AES-CCM (A3853)	128, 192, 256 bit keys, 128-bit IVs, encrypt	КАТ	CAST	Module becomes operational and services are available for use	Encryption	Test runs at power-on before the integrity test
AES-CCM (A3854)	128, 192, 256 bit keys, 128-bit IVs, encrypt	КАТ	CAST	Module becomes operational and services are available for use	Encryption	Test runs at power-on before the integrity test

Algorithm or Test	Test Properties	Test Method	Test	Indicator	Details	Conditions
AES-CCM (A3814)	128, 192, 256 bit keys, 128-bit IVs, decrypt	KAT	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-CCM (A3822)	128, 192, 256 bit keys, 128-bit IVs, decrypt	КАТ	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-CCM (A3829)	128, 192, 256 bit keys, 128-bit IVs, decrypt	КАТ	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-CCM (A3832)	128, 192, 256 bit keys, 128-bit IVs, decrypt	КАТ	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-CCM (A3843)	128, 192, 256 bit keys, 128-bit IVs, decrypt	КАТ	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-CCM (A3853)	128, 192, 256 bit keys, 128-bit IVs, decrypt	KAT	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-CCM (A3854)	128, 192, 256 bit keys, 128-bit IVs, decrypt	КАТ	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-GCM (A3814)	128, 192, 256 bit keys, 96-bit (internal IV), encrypt	КАТ	CAST	Module becomes operational and services are available for use	Encryption	Test runs at power-on before the integrity test
AES-GCM (A3820)	128, 192, 256 bit keys, 96-bit (internal IV), encrypt	КАТ	CAST	Module becomes operational and services are available for use	Encryption	Test runs at power-on before the integrity test
AES-GCM (A3821)	128, 192, 256 bit keys, 96-bit (internal IV), encrypt	КАТ	CAST	Module becomes operational and services are available for use	Encryption	Test runs at power-on before the integrity test
AES-GCM (A3822)	128, 192, 256 bit keys, 96-bit (internal IV), encrypt	KAT	CAST	Module becomes operational and	Encryption	Test runs at power-on

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				services are available for use		before the integrity test
AES-GCM (A3824)	128, 192, 256 bit keys, 96-bit (internal IV), encrypt	КАТ	CAST	Module becomes operational and services are available for use	Encryption	Test runs at power-on before the integrity test
AES-GCM (A3825)	128, 192, 256 bit keys, 96-bit (internal IV), encrypt	КАТ	CAST	Module becomes operational and services are available for use	Encryption	Test runs at power-on before the integrity test
AES-GCM (A3829)	128, 192, 256 bit keys, 96-bit (internal IV), encrypt	КАТ	CAST	Module becomes operational and services are available for use	Encryption	Test runs at power-on before the integrity test
AES-GCM (A3830)	128, 192, 256 bit keys, 96-bit (internal IV), encrypt	КАТ	CAST	Module becomes operational and services are available for use	Encryption	Test runs at power-on before the integrity test
AES-GCM (A3831)	128, 192, 256 bit keys, 96-bit (internal IV), encrypt	КАТ	CAST	Module becomes operational and services are available for use	Encryption	Test runs at power-on before the integrity test
AES-GCM (A3832)	128, 192, 256 bit keys, 96-bit (internal IV), encrypt	КАТ	CAST	Module becomes operational and services are available for use	Encryption	Test runs at power-on before the integrity test
AES-GCM (A3833)	128, 192, 256 bit keys, 96-bit (internal IV), encrypt	КАТ	CAST	Module becomes operational and services are available for use	Encryption	Test runs at power-on before the integrity test
AES-GCM (A3834)	128, 192, 256 bit keys, 96-bit (internal IV), encrypt	КАТ	CAST	Module becomes operational and services are available for use	Encryption	Test runs at power-on before the integrity test
AES-GCM (A3840)	128, 192, 256 bit keys, 96-bit (internal IV), encrypt	KAT	CAST	Module becomes operational and services are available for use	Encryption	Test runs at power-on before the integrity test
AES-GCM (A3841)	128, 192, 256 bit keys, 96-bit (internal IV), encrypt	КАТ	CAST	Module becomes operational and services are available for use	Encryption	Test runs at power-on before the integrity test

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-GCM (A3842)	128, 192, 256 bit keys, 96-bit (internal IV), encrypt	КАТ	CAST	Module becomes operational and services are available for use	Encryption	Test runs at power-on before the integrity test
AES-GCM (A3843)	128, 192, 256 bit keys, 96-bit (internal IV), encrypt	КАТ	CAST	Module becomes operational and services are available for use	Encryption	Test runs at power-on before the integrity test
AES-GCM (A3844)	128, 192, 256 bit keys, 96-bit (internal IV), encrypt	КАТ	CAST	Module becomes operational and services are available for use	Encryption	Test runs at power-on before the integrity test
AES-GCM (A3845)	128, 192, 256 bit keys, 96-bit (internal IV), encrypt	KAT	CAST	Module becomes operational and services are available for use	Encryption	Test runs at power-on before the integrity test
AES-GCM (A3854)	128, 192, 256 bit keys, 96-bit (internal IV), encrypt	KAT	CAST	Module becomes operational and services are available for use	Encryption	Test runs at power-on before the integrity test
AES-GCM (A3855)	128, 192, 256 bit keys, 96-bit (internal IV), encrypt	KAT	CAST	Module becomes operational and services are available for use	Encryption	Test runs at power-on before the integrity test
AES-GCM (A3856)	128, 192, 256 bit keys, 96-bit (internal IV), encrypt	КАТ	CAST	Module becomes operational and services are available for use	Encryption	Test runs at power-on before the integrity test
AES-GCM (A3814)	128, 192, 256 bit keys, 96-bit (internal IV), decrypt	КАТ	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-GCM (A3820)	128, 192, 256 bit keys, 96-bit (internal IV), decrypt	КАТ	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-GCM (A3821)	128, 192, 256 bit keys, 96-bit (internal IV), decrypt	КАТ	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-GCM (A3822)	128, 192, 256 bit keys, 96-bit (internal IV), decrypt	KAT	CAST	Module becomes operational and	Decryption	Test runs at power-on

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				services are available for use		before the integrity test
AES-GCM (A3824)	128, 192, 256 bit keys, 96-bit (internal IV), decrypt	КАТ	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-GCM (A3825)	128, 192, 256 bit keys, 96-bit (internal IV), decrypt	КАТ	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-GCM (A3829)	128, 192, 256 bit keys, 96-bit (internal IV), decrypt	КАТ	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-GCM (A3830)	128, 192, 256 bit keys, 96-bit (internal IV), decrypt	КАТ	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-GCM (A3831)	128, 192, 256 bit keys, 96-bit (internal IV), decrypt	КАТ	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-GCM (A3832)	128, 192, 256 bit keys, 96-bit (internal IV), decrypt	КАТ	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-GCM (A3833)	128, 192, 256 bit keys, 96-bit (internal IV), decrypt	КАТ	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-GCM (A3834)	128, 192, 256 bit keys, 96-bit (internal IV), decrypt	КАТ	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-GCM (A3840)	128, 192, 256 bit keys, 96-bit (internal IV), decrypt	KAT	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-GCM (A3841)	128, 192, 256 bit keys, 96-bit (internal IV), decrypt	КАТ	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test

Algorithm or	Test Properties	Test Method	Test	Indicator	Details	Conditions
AES-GCM (A3842)	128, 192, 256 bit keys, 96-bit (internal IV), decrypt	КАТ	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-GCM (A3843)	128, 192, 256 bit keys, 96-bit (internal IV), decrypt	КАТ	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-GCM (A3844)	128, 192, 256 bit keys, 96-bit (internal IV), decrypt	КАТ	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-GCM (A3845)	128, 192, 256 bit keys, 96-bit (internal IV), decrypt	КАТ	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-GCM (A3854)	128, 192, 256 bit keys, 96-bit (internal IV), decrypt	КАТ	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-GCM (A3855)	128, 192, 256 bit keys, 96-bit (internal IV), decrypt	КАТ	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-GCM (A3856)	128, 192, 256 bit keys, 96-bit (internal IV), decrypt	КАТ	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-OFB (A3818)	128 bit keys, encrypt	КАТ	CAST	Module becomes operational and services are available for use	Encryption	Test runs at power-on before the integrity test
AES-OFB (A3827)	128 bit keys, encrypt	КАТ	CAST	Module becomes operational and services are available for use	Encryption	Test runs at power-on before the integrity test
AES-OFB (A3837)	128 bit keys, encrypt	KAT	CAST	Module becomes operational and services are available for use	Encryption	Test runs at power-on before the integrity test
AES-OFB (A3848)	128 bit keys, encrypt	КАТ	CAST	Module becomes operational and	Encryption	Test runs at power-on

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
			Type	services are available for use		before the integrity test
AES-OFB (A3854)	128 bit keys, encrypt	КАТ	CAST	Module becomes operational and services are available for use	Encryption	Test runs at power-on before the integrity test
AES-OFB (A3818)	128 bit keys, decrypt	КАТ	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-OFB (A3827)	128 bit keys, decrypt	КАТ	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-OFB (A3837)	128 bit keys, decrypt	КАТ	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-OFB (A3848)	128 bit keys, decrypt	КАТ	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-OFB (A3854)	128 bit keys, decrypt	КАТ	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-XTS Testing Revision 2.0 (A3814)	128 and 256 bit keys, encrypt	КАТ	CAST	Module becomes operational and services are available for use	Encryption	Test runs at power-on before the integrity test
AES-XTS Testing Revision 2.0 (A3822)	128 and 256 bit keys, encrypt	КАТ	CAST	Module becomes operational and services are available for use	Encryption	Test runs at power-on before the integrity test
AES-XTS Testing Revision 2.0 (A3829)	128 and 256 bit keys, encrypt	КАТ	CAST	Module becomes operational and services are available for use	Encryption	Test runs at power-on before the integrity test
AES-XTS Testing Revision 2.0 (A3832)	128 and 256 bit keys, encrypt	КАТ	CAST	Module becomes operational and services are available for use	Encryption	Test runs at power-on before the integrity test

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-XTS	128 and 256 hit keys	ΚΔΤ	CAST	Module	Encryption	Test runs at
Testing	encrypt		CASI	hecomes		
Revision 2.0	enerype			operational and		before the
(A 3840)				services are		integrity test
(7.50-10)				available for use		
AES-XTS	128 and 256 bit keys,	KAT	CAST	Module	Encryption	Test runs at
Testing	encrypt			becomes		power-on
Revision 2.0				operational and		before the
(A3843)				services are		integrity test
				available for use		
AES-XTS	128 and 256 bit keys,	KAT	CAST	Module	Encryption	Test runs at
Testing	encrypt			becomes		power-on
Revision 2.0				operational and		before the
(A3853)				services are		integrity test
				available for use		
AES-XTS	128 and 256 bit keys,	KAT	CAST	Module	Encryption	Test runs at
Testing	encrypt			becomes		power-on
Revision 2.0				operational and		before the
(A3854)				services are		integrity test
				available for use		
AES-XTS	128 and 256 bit keys,	KAT	CAST	Module	Encryption	Test runs at
Testing	encrypt			becomes		power-on
Revision 2.0				operational and		before the
(A3857)				services are		integrity test
				available for use		
AES-XTS	128 and 256 bit keys,	KAT	CAST	Module	Decryption	Test runs at
Testing	decrypt			becomes		power-on
Revision 2.0				operational and		before the
(A3814)				services are		integrity test
				available for use		
AES-XIS	128 and 256 bit keys,	KAT	CASI	Module	Decryption	lest runs at
Testing	aecrypt			Decomes		power-on
Revision 2.0				operational and		
(A3822)				services are		incegrity test
			CACT	available for use	Description	T
AES-XIS	128 and 256 DIC Keys,	KAT	CASI	Module	Decryption	Test runs at
Devision 2.0	decrypt			Decomes		power-on
(A3829)						integrity test
	128 and 256 hit kove	KAT	Слет	Modulo	Decryption	Tost sups at
			CASI	hecomes	Deciyption	
Povision 2.0	deciypt			operational and		boforo tho
(12832)						integrity test
(A3032)				available for use		integrity test
ΔΕς-ΧΤς	128 and 256 hit keys	κάτ	СДСТ	Module	Decryption	Test runs at
Testing	decrypt			hecomes		
Revision 20				operational and		before the
(A 3840)						integrity test
,,				available for use		incegney cese
ΔΕς-ΧΤς	128 and 256 hit keys	ΚΔΤ	СДСТ	Module	Decryption	Test runs at
Testing	decrypt			becomes		Dower-on
				operational and		F

Algorithm or Test	Test Properties	Test Method	Test Tvpe	Indicator	Details	Conditions
Revision 2.0 (A3843)				services are available for use		before the integrity test
AES-XTS Testing Revision 2.0 (A3853)	128 and 256 bit keys, decrypt	КАТ	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-XTS Testing Revision 2.0 (A3854)	128 and 256 bit keys, decrypt	КАТ	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-XTS Testing Revision 2.0 (A3857)	128 and 256 bit keys, decrypt	КАТ	CAST	Module becomes operational and services are available for use	Decryption	Test runs at power-on before the integrity test
AES-CMAC (A3814)	128 and 256 bit keys, encrypt	КАТ	CAST	Module becomes operational and services are available for use	Message authentication	Test runs at power-on before the integrity test
AES-CMAC (A3822)	128 and 256 bit keys, encrypt	КАТ	CAST	Module becomes operational and services are available for use	Message authentication	Test runs at power-on before the integrity test
AES-CMAC (A3829)	128 and 256 bit keys, encrypt	КАТ	CAST	Module becomes operational and services are available for use	Message authentication	Test runs at power-on before the integrity test
AES-CMAC (A3832)	128 and 256 bit keys, encrypt	КАТ	CAST	Module becomes operational and services are available for use	Message authentication	Test runs at power-on before the integrity test
AES-CMAC (A3843)	128 and 256 bit keys, encrypt	КАТ	CAST	Module becomes operational and services are available for use	Message authentication	Test runs at power-on before the integrity test
AES-CMAC (A3853)	128 and 256 bit keys, encrypt	КАТ	CAST	Module becomes operational and services are available for use	Message authentication	Test runs at power-on before the integrity test
AES-CMAC (A3854)	128 and 256 bit keys, encrypt	КАТ	CAST	Module becomes operational and services are available for use	Message authentication	Test runs at power-on before the integrity test

Algorithm or Test	Test Properties	Test Method	Test Tvpe	Indicator	Details	Conditions
SHA-1 (A3812)	SHA-1	КАТ	CAST	Module becomes operational and services are available for use	Message digest	Test runs at power-on before the integrity test
SHA-1 (A3813)	SHA-1	КАТ	CAST	Module becomes operational and services are available for use	Message digest	Test runs at power-on before the integrity test
SHA-1 (A3814)	SHA-1	КАТ	CAST	Module becomes operational and services are available for use	Message digest	Test runs at power-on before the integrity test
SHA-1 (A3832)	SHA-1	КАТ	CAST	Module becomes operational and services are available for use	Message digest	Test runs at power-on before the integrity test
SHA-1 (A3850)	SHA-1	КАТ	CAST	Module becomes operational and services are available for use	Message digest	Test runs at power-on before the integrity test
SHA-1 (A3851)	SHA-1	KAT	CAST	Module becomes operational and services are available for use	Message digest	Test runs at power-on before the integrity test
SHA-1 (A3852)	SHA-1	КАТ	CAST	Module becomes operational and services are available for use	Message digest	Test runs at power-on before the integrity test
SHA-1 (A3853)	SHA-1	КАТ	CAST	Module becomes operational and services are available for use	Message digest	Test runs at power-on before the integrity test
SHA2-224 (A3812)	SHA2-224	КАТ	CAST	Module becomes operational and services are available for use	Message digest	Test runs at power-on before the integrity test
SHA2-224 (A3813)	SHA2-224	KAT	CAST	Module becomes operational and services are available for use	Message digest	Test runs at power-on before the integrity test
SHA2-224 (A3814)	SHA2-224	КАТ	CAST	Module becomes operational and	Message digest	Test runs at power-on

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

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

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				services are available for use		before the integrity test
SHA2-384 (A3850)	SHA2-384	КАТ	CAST	Module becomes operational and services are available for use	Message digest	Test runs at power-on before the integrity test
SHA2-384 (A3851)	SHA2-384	КАТ	CAST	Module becomes operational and services are available for use	Message digest	Test runs at power-on before the integrity test
SHA2-384 (A3852)	SHA2-384	КАТ	CAST	Module becomes operational and services are available for use	Message digest	Test runs at power-on before the integrity test
SHA2-384 (A3858)	SHA2-384	КАТ	CAST	Module becomes operational and services are available for use	Message digest	Test runs at power-on before the integrity test
SHA2-512 (A3812)	SHA2-512	KAT	CAST	Module becomes operational and services are available for use	Message digest	Test runs at power-on before the integrity test
SHA2-512 (A3813)	SHA2-512	КАТ	CAST	Module becomes operational and services are available for use	Message digest	Test runs at power-on before the integrity test
SHA2-512 (A3814)	SHA2-512	КАТ	CAST	Module becomes operational and services are available for use	Message digest	Test runs at power-on before the integrity test
SHA2-512 (A3832)	SHA2-512	КАТ	CAST	Module becomes operational and services are available for use	Message digest	Test runs at power-on before the integrity test
SHA2-512 (A3850)	SHA2-512	KAT	CAST	Module becomes operational and services are available for use	Message digest	Test runs at power-on before the integrity test
SHA2-512 (A3851)	SHA2-512	KAT	CAST	Module becomes operational and services are available for use	Message digest	Test runs at power-on before the integrity test

Algorithm or Test	Test Properties	Test Method	Test	Indicator	Details	Conditions
SHA2-512 (A3852)	SHA2-512	KAT	CAST	Module becomes operational and services are available for use	Message digest	Test runs at power-on before the integrity test
SHA2-512 (A3858)	SHA2-512	КАТ	CAST	Module becomes operational and services are available for use	Message digest	Test runs at power-on before the integrity test
SHA3-224 (A3816)	SHA3-224	КАТ	CAST	Module becomes operational and services are available for use	Message digest	Test runs at power-on before the integrity test
SHA3-224 (A3839)	SHA3-224	КАТ	CAST	Module becomes operational and services are available for use	Message digest	Test runs at power-on before the integrity test
SHA3-256 (A3816)	SHA3-256	КАТ	CAST	Module becomes operational and services are available for use	Message digest	Test runs at power-on before the integrity test
SHA3-256 (A3839)	SHA3-256	КАТ	CAST	Module becomes operational and services are available for use	Message digest	Test runs at power-on before the integrity test
SHA3-384 (A3816)	SHA3-384	КАТ	CAST	Module becomes operational and services are available for use	Message digest	Test runs at power-on before the integrity test
SHA3-384 (A3839)	SHA3-384	КАТ	CAST	Module becomes operational and services are available for use	Message digest	Test runs at power-on before the integrity test
SHA3-512 (A3816)	SHA3-512	КАТ	CAST	Module becomes operational and services are available for use	Message digest	Test runs at power-on before the integrity test
SHA3-512 (A3839)	SHA3-512	КАТ	CAST	Module becomes operational and services are available for use	Message digest	Test runs at power-on before the integrity test
HMAC-SHA-1 (A3812)	SHA-1	КАТ	CAST	Module becomes operational and	Message authentication	Test runs at power-on

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				services are available for use		before the integrity test
HMAC-SHA-1 (A3813)	SHA-1	КАТ	CAST	Module becomes operational and services are available for use	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA-1 (A3814)	SHA-1	КАТ	CAST	Module becomes operational and services are available for use	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA-1 (A3832)	SHA-1	КАТ	CAST	Module becomes operational and services are available for use	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA-1 (A3850)	SHA-1	КАТ	CAST	Module becomes operational and services are available for use	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA-1 (A3851)	SHA-1	КАТ	CAST	Module becomes operational and services are available for use	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA-1 (A3852)	SHA-1	КАТ	CAST	Module becomes operational and services are available for use	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA-1 (A3853)	SHA-1	КАТ	CAST	Module becomes operational and services are available for use	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2- 224 (A3812)	SHA2-224	КАТ	CAST	Module becomes operational and services are available for use	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2- 224 (A3813)	SHA2-224	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2- 224 (A3814)	SHA2-224	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Test runs at power-on before the integrity test
Algorithm or	Test Properties	Test Method	Test	Indicator	Details	Conditions
---------------	-----------------	----------------	-------	-------------------	----------------	-------------------
	CUAD 224	Mechou MAT	САСТ	Madula	Massaga	Test supe at
11MAC-30AZ-	3NAZ-224	NAT	CAST	hocomes	authentication	
224 (A3652)				operational and		bofoso the
				operational and		intogrity tost
				services are		integrity test
	CUAD 224	VAT	CAST	Available for use	Massaga	Test supe at
	3NAZ-224	NAT	CAST	hasamas	Message	
224 (A3650)				Decomes	authentication	power-on
						intogrity toot
						integrity test
	CUAD 224	VAT	CAST	Available for use	Massaga	Test supe at
	SHAZ-224	KAT	CASI	Module	Message	Test Turis at
224 (A3651)				Decomes	authentication	power-on
				operacional and		istocity tost
						integrity test
	CU A 2 224		CACT	available for use		Testaures
	SHAZ-ZZ4	KAT	CAST	Module	Message	Test runs at
224 (A3852)				Decomes	authentication	power-on
				operacional and		is to asily to at
						integrity test
	CUAD 224	VAT	CAST	Available for use	Massaga	Test supe at
111/1AC-30AZ-	5HAZ-224	NAT	CAST	hocomos	Message	
224 (A3633)				Decomes	authentication	bofoso the
				operacional and		istocity tost
				services are		integrity test
	CUAD 224	V AT	CAST	Modulo	Mossago	Tost supe at
11MAC-30AZ-	3NAZ-224	NAT	CAST	hocomos	nessage	
224 (A3637)				operational and	authentication	boforo the
						integrity test
				available for use		integrity test
	SHV3-334	клт	СЛСТ	Module	Message	Test runs at
224 (A3858)	JI IAZ-224		CASI	hecomes	authentication	
224 (A3030)				operational and		before the
						integrity test
				available for use		incegney cese
ΗΜΔΟ-ΣΗΔ2-	SHA2-256	κΔΤ	CAST	Module	Message	Test runs at
256 (A3812)	STIAL 250		CASI	becomes	authentication	
250 (/(5012)				operational and	detrendedelori	before the
				services are		integrity test
				available for use		incegney cese
HMAC-SHA2-	SHA2-256	ΚΑΤ	CAST	Module	Message	Test runs at
256 (A3813)			0/101	becomes	authentication	power-on
				operational and		before the
				services are		integrity test
				available for use		5,5
HMAC-SHA2-	SHA2-256	КАТ	CAST	Module	Message	Test runs at
256 (A3814)				becomes	authentication	power-on
				operational and		before the
				services are		integrity test
				available for use		
HMAC-SHA2-	SHA2-256	КАТ	CAST	Module	Message	Test runs at
256 (A3832)				becomes	authentication	power-on
				operational and		

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

Algorithm or	Test Properties	Test Method	Test	Indicator	Details	Conditions
	CUAD 204		САСТ	Modulo	Mossago	Tost supe at
10/AC-30AZ-	3NA2-304	NAT	CAST	hocomes	authentication	
564 (A3650)				operational and		bofoso the
				operational and		intogrity tost
				services are		integrity test
		VAT	CAST	Available for use	Massaga	Test supe at
	3NA2-304	NAT	CAST	hasamas	Message	
364 (A3631)				Decomes	authentication	power-on
						intogrity toot
						integrity test
	CUAD 204		CACT	available for use		Testaures
HMAC-SHAZ-	SHAZ-384	KAT	CASI	Module	Message	Test runs at
384 (A3852)				Decomes	authentication	power-on
				operational and		berore the
						integrity test
	CU 4 2 204		CACT	available for use	N 4	T b b
HMAC-SHAZ-	SHAZ-384	KAT	CAST	Module	Message	lest runs at
384 (A3858)				Decomes	authentication	power-on
				operational and		
				services are		integrity test
	CU 4 0 540		CACT	available ror use		-
HMAC-SHAZ-	SHAZ-512	KAT	CAST	Module	Message	lest runs at
512 (A3812)				Decomes	authentication	power-on
				operational and		before the
				services are		integrity test
		IX A T	CACT	available for use		-
HMAC-SHA2-	SHAZ-512	KAT	CAST	Module	Message	lest runs at
512 (A3813)				becomes	authentication	power-on
				operational and		before the
				services are		integrity test
				available for use		
HMAC-SHA2-	SHA2-512	KAT	CAST	Module	Message	Test runs at
512 (A3814)				becomes	authentication	power-on
				operational and		before the
				services are		integrity test
				available for use		
HMAC-SHA2-	SHA2-512	KAT	CAST	Module	Message	lest runs at
512 (A3832)				becomes	authentication	power-on
				operational and		
				services are		integrity test
	CU 4 0 540		CACT	available ror use		-
HMAC-SHAZ-	SHAZ-512	KAT	CAST	Module	Message	lest runs at
512 (A3850)				Decomes	authentication	power-on
				operational and		before the
				services are		integrity test
			C 4 C -	available for use		T
HMAC-SHA2-	SHA2-512	KAT	CAST	Module	Message	lest runs at
512 (A3851)				becomes	authentication	power-on
				operational and		Defore the
				services are		integrity test
			<u></u>	available for use		- · ·
HMAC-SHA2-	SHA2-512	KAT	CAST	Module	Message	lest runs at
512 (A3852)				becomes	authentication	power-on
1	1	1	1	Ioperational and	1	

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
			Type	services are available for use		before the integrity test
HMAC-SHA2- 512 (A3858)	SHA2-512	КАТ	CAST	Module becomes operational and services are available for use	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA3- 224 (A3816)	SHA3-224	КАТ	CAST	Module becomes operational and services are available for use	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA3- 224 (A3839)	SHA3-224	КАТ	CAST	Module becomes operational and services are available for use	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA3- 256 (A3816)	SHA3-256	КАТ	CAST	Module becomes operational and services are available for use	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA3- 256 (A3839)	SHA3-256	КАТ	CAST	Module becomes operational and services are available for use	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA3- 384 (A3816)	SHA3-384	КАТ	CAST	Module becomes operational and services are available for use	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA3- 384 (A3839)	SHA3-384	КАТ	CAST	Module becomes operational and services are available for use	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA3- 512 (A3816)	SHA3-512	КАТ	CAST	Module becomes operational and services are available for use	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA3- 512 (A3839)	SHA3-512	КАТ	CAST	Module becomes operational and services are available for use	Message authentication	Test runs at power-on before the integrity test
Counter DRBG (A3812)	128, 192, 256 bit keys, with/without PR	KAT	CAST	Module becomes operational and services are available for use	SP800-90Arev1 health test	Test runs at power-on before the integrity test

ubuntu[©]Canonical Ltd. Ubuntu 22.04 Kernel Crypto API Cryptographic Module FIPS 140-3 Non-Proprietary Security Policy

Algorithm or	Test Properties	Test Method	Test	Indicator	Details	Conditions
Counter DRBG (A3813)	128, 192, 256 bit keys, with/without PR	KAT	CAST	Module becomes operational and services are available for use	SP800-90Arev1 health test	Test runs at power-on before the integrity test
Counter DRBG (A3814)	128, 192, 256 bit keys, with/without PR	КАТ	CAST	Module becomes operational and services are available for use	SP800-90Arev1 health test	Test runs at power-on before the integrity test
Counter DRBG (A3820)	128, 192, 256 bit keys, with/without PR	КАТ	CAST	Module becomes operational and services are available for use	SP800-90Arev1 health test	Test runs at power-on before the integrity test
Counter DRBG (A3821)	128, 192, 256 bit keys, with/without PR	КАТ	CAST	Module becomes operational and services are available for use	SP800-90Arev1 health test	Test runs at power-on before the integrity test
Counter DRBG (A3822)	128, 192, 256 bit keys, with/without PR	КАТ	CAST	Module becomes operational and services are available for use	SP800-90Arev1 health test	Test runs at power-on before the integrity test
Counter DRBG (A3824)	128, 192, 256 bit keys, with/without PR	КАТ	CAST	Module becomes operational and services are available for use	SP800-90Arev1 health test	Test runs at power-on before the integrity test
Counter DRBG (A3825)	128, 192, 256 bit keys, with/without PR	КАТ	CAST	Module becomes operational and services are available for use	SP800-90Arev1 health test	Test runs at power-on before the integrity test
Counter DRBG (A3829)	128, 192, 256 bit keys, with/without PR	КАТ	CAST	Module becomes operational and services are available for use	SP800-90Arev1 health test	Test runs at power-on before the integrity test
Counter DRBG (A3830)	128, 192, 256 bit keys, with/without PR	КАТ	CAST	Module becomes operational and services are available for use	SP800-90Arev1 health test	Test runs at power-on before the integrity test
Counter DRBG (A3831)	128, 192, 256 bit keys, with/without PR	КАТ	CAST	Module becomes operational and services are available for use	SP800-90Arev1 health test	Test runs at power-on before the integrity test
Counter DRBG (A3832)	128, 192, 256 bit keys, with/without PR	КАТ	CAST	Module becomes operational and	SP800-90Arev1 health test	Test runs at power-on

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				services are available for use		before the integrity test
Counter DRBG (A3833)	128, 192, 256 bit keys, with/without PR	KAT	CAST	Module becomes operational and services are available for use	SP800-90Arev1 health test	Test runs at power-on before the integrity test
Counter DRBG (A3834)	128, 192, 256 bit keys, with/without PR	КАТ	CAST	Module becomes operational and services are available for use	SP800-90Arev1 health test	Test runs at power-on before the integrity test
Counter DRBG (A3840)	128, 192, 256 bit keys, with/without PR	КАТ	CAST	Module becomes operational and services are available for use	SP800-90Arev1 health test	Test runs at power-on before the integrity test
Counter DRBG (A3841)	128, 192, 256 bit keys, with/without PR	КАТ	CAST	Module becomes operational and services are available for use	SP800-90Arev1 health test	Test runs at power-on before the integrity test
Counter DRBG (A3842)	128, 192, 256 bit keys, with/without PR	КАТ	CAST	Module becomes operational and services are available for use	SP800-90Arev1 health test	Test runs at power-on before the integrity test
Counter DRBG (A3843)	128, 192, 256 bit keys, with/without PR	КАТ	CAST	Module becomes operational and services are available for use	SP800-90Arev1 health test	Test runs at power-on before the integrity test
Counter DRBG (A3844)	128, 192, 256 bit keys, with/without PR	КАТ	CAST	Module becomes operational and services are available for use	SP800-90Arev1 health test	Test runs at power-on before the integrity test
Counter DRBG (A3845)	128, 192, 256 bit keys, with/without PR	КАТ	CAST	Module becomes operational and services are available for use	SP800-90Arev1 health test	Test runs at power-on before the integrity test
Counter DRBG (A3854)	128, 192, 256 bit keys, with/without PR	КАТ	CAST	Module becomes operational and services are available for use	SP800-90Arev1 health test	Test runs at power-on before the integrity test
Counter DRBG (A3855)	128, 192, 256 bit keys, with/without PR	KAT	CAST	Module becomes operational and services are available for use	SP800-90Arev1 health test	Test runs at power-on before the integrity test

ubuntu⁹Canonical Ltd. Ubuntu 22.04 Kernel Crypto API Cryptographic Module FIPS 140-3 Non-Proprietary Security Policy

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
Counter	128 192 256 hit	КАТ	CAST	Module		Test runs at
	kevs with/without		CASI	hecomes	health test	
(13856)				operational and		before the
(A3030)	FIN					integrity test
				available for use		
Hash DRBG	SHA2-256	KAT	CAST	Module	SP800-90Arev1	Test runs at
(A3812)	With/without PR			becomes	health test	power-on
				operational and		before the
				services are		integrity test
				available for use		
Hash DRBG	SHA2-256	KAT	CAST	Module	SP800-90Arev1	Test runs at
(A3813)	With/without PR			becomes	health test	power-on
				operational and		before the
				services are		integrity test
				available for use		
Hash DRBG	SHA2-256	KAT	CAST	Module	SP800-90Arev1	Test runs at
(A3814)	With/without PR			becomes	health test	power-on
				operational and		before the
				services are		integrity test
				available for use		
Hash DRBG	SHA2-256	KAT	CAST	Module	SP800-90Arev1	Test runs at
(A3820)	With/without PR			becomes	health test	power-on
				operational and		before the
				services are		integrity test
				available for use		
Hash DRBG	SHA2-256	KAT	CAST	Module	SP800-90Arev1	Test runs at
(A3821)	With/without PR			becomes	health test	power-on
				operational and		before the
				services are		integrity test
	<u> </u>		<u></u>	available for use		
Hash DRBG	SHA2-256	KAT	CAST	Module	SP800-90Arev1	lest runs at
(A3822)	WITH/WITHOUT PR			becomes	nealth test	power-on
				operational and		Derore the
				services are		incegrity test
			CACT	available for use		Techauseeb
	SHAZ-250	KAT	CASI	hoodule	SP800-90ATEVT	Test Turis at
(A3624)				operational and		power-on
				services are		integrity test
	CUAD 256	V AT	CAST	Modulo	SD800.004 cov1	Tost supe at
(A 3825)	With/without PR		CASI	hecomes	health test	
(A3023)				operational and		before the
						integrity test
				available for use		integrity test
Hash DRBG	SHA2-256	КАТ	СДСТ	Module	SP800-90Δrev1	Test runs at
(43830)	With/without PR	1011	0/101	hecomes	health test	
(43030)				operational and		before the
				services are		integrity test
				available for use		
Hash DRBG	SHA2-256	КАТ	СДСТ	Module	SP800-90Δrev1	Test runs at
(A3831)	With/without PR		0,01	becomes	health test	power-on
,,				operational and		

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				services are available for use		before the integrity test
Hash DRBG (A3832)	SHA2-256 With/without PR	КАТ	CAST	Module becomes operational and services are available for use	SP800-90Arev1 health test	Test runs at power-on before the integrity test
Hash DRBG (A3833)	SHA2-256 With/without PR	КАТ	CAST	Module becomes operational and services are available for use	SP800-90Arev1 health test	Test runs at power-on before the integrity test
Hash DRBG (A3834)	SHA2-256 With/without PR	КАТ	CAST	Module becomes operational and services are available for use	SP800-90Arev1 health test	Test runs at power-on before the integrity test
Hash DRBG (A3840)	SHA2-256 With/without PR	КАТ	CAST	Module becomes operational and services are available for use	SP800-90Arev1 health test	Test runs at power-on before the integrity test
Hash DRBG (A3841)	SHA2-256 With/without PR	КАТ	CAST	Module becomes operational and services are available for use	SP800-90Arev1 health test	Test runs at power-on before the integrity test
Hash DRBG (A3842)	SHA2-256 With/without PR	КАТ	CAST	Module becomes operational and services are available for use	SP800-90Arev1 health test	Test runs at power-on before the integrity test
Hash DRBG (A3843)	SHA2-256 With/without PR	КАТ	CAST	Module becomes operational and services are available for use	SP800-90Arev1 health test	Test runs at power-on before the integrity test
Hash DRBG (A3844)	SHA2-256 With/without PR	КАТ	CAST	Module becomes operational and services are available for use	SP800-90Arev1 health test	Test runs at power-on before the integrity test
Hash DRBG (A3845)	SHA2-256 With/without PR	КАТ	CAST	Module becomes operational and services are available for use	SP800-90Arev1 health test	Test runs at power-on before the integrity test
Hash DRBG (A3850)	SHA2-256 With/without PR	КАТ	CAST	Module becomes operational and services are available for use	SP800-90Arev1 health test	Test runs at power-on before the integrity test

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
Hash DRBG (A3851)	SHA2-256 With/without PR	КАТ	CAST	Module becomes operational and services are	SP800-90Arev1 health test	Test runs at power-on before the integrity test
Hash DRBG (A3852)	SHA2-256 With/without PR	КАТ	CAST	available for use Module becomes operational and services are available for use	SP800-90Arev1 health test	Test runs at power-on before the integrity test
Hash DRBG (A3855)	SHA2-256 With/without PR	КАТ	CAST	Module becomes operational and services are available for use	SP800-90Arev1 health test	Test runs at power-on before the integrity test
Hash DRBG (A3856)	SHA2-256 With/without PR	КАТ	CAST	Module becomes operational and services are available for use	SP800-90Arev1 health test	Test runs at power-on before the integrity test
HMAC DRBG (A3812)	HMAC-SHA2-256, HMAC-SHA2-512, with/without PR	КАТ	CAST	Module becomes operational and services are available for use	SP800-90Arev1 health test	Test runs at power-on before the integrity test
HMAC DRBG (A3813)	HMAC-SHA2-256, HMAC-SHA2-512, with/without PR	КАТ	CAST	Module becomes operational and services are available for use	SP800-90Arev1 health test	Test runs at power-on before the integrity test
HMAC DRBG (A3814)	HMAC-SHA2-256, HMAC-SHA2-512, with/without PR	КАТ	CAST	Module becomes operational and services are available for use	SP800-90Arev1 health test	Test runs at power-on before the integrity test
HMAC DRBG (A3820)	HMAC-SHA2-256, HMAC-SHA2-512, with/without PR	КАТ	CAST	Module becomes operational and services are available for use	SP800-90Arev1 health test	Test runs at power-on before the integrity test
HMAC DRBG (A3821)	HMAC-SHA2-256, HMAC-SHA2-512, with/without PR	КАТ	CAST	Module becomes operational and services are available for use	SP800-90Arev1 health test	Test runs at power-on before the integrity test
HMAC DRBG (A3822)	HMAC-SHA2-256, HMAC-SHA2-512, with/without PR	KAT	CAST	Module becomes operational and services are available for use	SP800-90Arev1 health test	Test runs at power-on before the integrity test
HMAC DRBG (A3824)	HMAC-SHA2-256, HMAC-SHA2-512, with/without_PR	КАТ	CAST	Module becomes operational and	SP800-90Arev1 health test	Test runs at power-on

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
			Type	services are available for use		before the integrity test
HMAC DRBG (A3825)	HMAC-SHA2-256, HMAC-SHA2-512, with/without PR	КАТ	CAST	Module becomes operational and services are available for use	SP800-90Arev1 health test	Test runs at power-on before the integrity test
HMAC DRBG (A3830)	HMAC-SHA2-256, HMAC-SHA2-512, with/without PR	КАТ	CAST	Module becomes operational and services are available for use	SP800-90Arev1 health test	Test runs at power-on before the integrity test
HMAC DRBG (A3831)	HMAC-SHA2-256, HMAC-SHA2-512, with/without PR	КАТ	CAST	Module becomes operational and services are available for use	SP800-90Arev1 health test	Test runs at power-on before the integrity test
HMAC DRBG (A3832)	HMAC-SHA2-256, HMAC-SHA2-512, with/without PR	КАТ	CAST	Module becomes operational and services are available for use	SP800-90Arev1 health test	Test runs at power-on before the integrity test
HMAC DRBG (A3833)	HMAC-SHA2-256, HMAC-SHA2-512, with/without PR	КАТ	CAST	Module becomes operational and services are available for use	SP800-90Arev1 health test	Test runs at power-on before the integrity test
HMAC DRBG (A3834)	HMAC-SHA2-256, HMAC-SHA2-512, with/without PR	КАТ	CAST	Module becomes operational and services are available for use	SP800-90Arev1 health test	Test runs at power-on before the integrity test
HMAC DRBG (A3840)	HMAC-SHA2-256, HMAC-SHA2-512, with/without PR	KAT	CAST	Module becomes operational and services are available for use	SP800-90Arev1 health test	Test runs at power-on before the integrity test
HMAC DRBG (A3841)	HMAC-SHA2-256, HMAC-SHA2-512, with/without PR	КАТ	CAST	Module becomes operational and services are available for use	SP800-90Arev1 health test	Test runs at power-on before the integrity test
HMAC DRBG (A3842)	HMAC-SHA2-256, HMAC-SHA2-512, with/without PR	KAT	CAST	Module becomes operational and services are available for use	SP800-90Arev1 health test	Test runs at power-on before the integrity test
HMAC DRBG (A3843)	HMAC-SHA2-256, HMAC-SHA2-512, with/without PR	КАТ	CAST	Module becomes operational and services are available for use	SP800-90Arev1 health test	Test runs at power-on before the integrity test

ubuntu[©]Canonical Ltd. Ubuntu 22.04 Kernel Crypto API Cryptographic Module FIPS 140-3 Non-Proprietary Security Policy

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HMAC DRBG (A3844)	HMAC-SHA2-256, HMAC-SHA2-512, with/without PR	КАТ	CAST	Module becomes operational and services are available for use	SP800-90Arev1 health test	Test runs at power-on before the integrity test
HMAC DRBG (A3845)	HMAC-SHA2-256, HMAC-SHA2-512, with/without PR	KAT	CAST	Module becomes operational and services are available for use	SP800-90Arev1 health test	Test runs at power-on before the integrity test
HMAC DRBG (A3850)	HMAC-SHA2-256, HMAC-SHA2-512, with/without PR	КАТ	CAST	Module becomes operational and services are available for use	SP800-90Arev1 health test	Test runs at power-on before the integrity test
HMAC DRBG (A3851)	HMAC-SHA2-256, HMAC-SHA2-512, with/without PR	КАТ	CAST	Module becomes operational and services are available for use	SP800-90Arev1 health test	Test runs at power-on before the integrity test
HMAC DRBG (A3852)	HMAC-SHA2-256, HMAC-SHA2-512, with/without PR	КАТ	CAST	Module becomes operational and services are available for use	SP800-90Arev1 health test	Test runs at power-on before the integrity test
HMAC DRBG (A3855)	HMAC-SHA2-256, HMAC-SHA2-512, with/without PR	KAT	CAST	Module becomes operational and services are available for use	SP800-90Arev1 health test	Test runs at power-on before the integrity test
HMAC DRBG (A3856)	HMAC-SHA2-256, HMAC-SHA2-512, with/without PR	КАТ	CAST	Module becomes operational and services are available for use	SP800-90Arev1 health test	Test runs at power-on before the integrity test
KAS-ECC-SSC Sp800-56Ar3 (A3813)	P-256, P-384 curves	КАТ	CAST	Module becomes operational and services are available for use	Shared secret computation	Test runs at power-on before the integrity test
KAS-FFC-SSC Sp800-56Ar3 (A3812)	ffdhe2048	КАТ	CAST	Module becomes operational and services are available for use	Shared secret computation	Test runs at power-on before the integrity test
RSA SigVer (FIPS186-4) (A3814)	PKCS#1 v1.5 with 2048 bit key and SHA2-256	KAT	CAST	Module becomes operational and services are available for use	Digital signature verification	Test runs at power-on before the integrity test
RSA SigVer (FIPS186-4) (A3832)	PKCS#1 v1.5 with 2048 bit key and SHA2-256	KAT	CAST	Module becomes operational and	Digital signature verification	Test runs at power-on

Algorithm or	Test Properties	Test Method	Test	Indicator	Details	Conditions
Test		Mechod	туре	services are available for use		before the integrity test
RSA SigVer (FIPS186-4) (A3850)	PKCS#1 v1.5 with 2048 bit key and SHA2-256	КАТ	CAST	Module becomes operational and services are available for use	Digital signature verification	Test runs at power-on before the integrity test
RSA SigVer (FIPS186-4) (A3851)	PKCS#1 v1.5 with 2048 bit key and SHA2-256	КАТ	CAST	Module becomes operational and services are available for use	Digital signature verification	Test runs at power-on before the integrity test
RSA SigVer (FIPS186-4) (A3852)	PKCS#1 v1.5 with 2048 bit key and SHA2-256	КАТ	CAST	Module becomes operational and services are available for use	Digital signature verification	Test runs at power-on before the integrity test
Safe Primes Key Generation (A3812)	ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192, Section 5.6.1.1.4 Testing Candidates	PCT	РСТ	Successful key pair generation	Signature generation & verification	Key pair generation
ECDSA KeyGen (FIPS186-4) (A3813)	SHA2-256, P-256, P- 384 curves, Appendix B.4.2 Testing Candidates	РСТ	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
Entropy Source	1024 samples	RCT	CAST	Module becomes operational and services are available for use	Entropy source startup test	Entropy source initialization
Entropy Source	1024 samples	ΑΡΤ	CAST	Module becomes operational and services are available for use	Entropy source startup test	Entropy source initialization
Entropy Source	Continuously	RCT	CAST	Entropy source is operational	Entropy source continuous test	Continuously
Entropy Source	Continuously	APT	CAST	Entropy source is operational	Entropy source continuous test	Continuously

Table 21: Conditional Self-Tests

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

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
HMAC-SHA2-256	Message	SW/FW Integrity	On Demand	Manually
(A3812)	Authentication			

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
HMAC-SHA2-256	Message	SW/FW Integrity	On Demand	Manually
(A3813)	Authentication	, 5,		2
HMAC-SHA2-256	Message	SW/FW Integrity	On Demand	Manually
(A3814)	Authentication			-
HMAC-SHA2-256	Message	SW/FW Integrity	On Demand	Manually
(A3832)	Authentication			-
HMAC-SHA2-256	Message	SW/FW Integrity	On Demand	Manually
(A3850)	Authentication			-
HMAC-SHA2-256	Message	SW/FW Integrity	On Demand	Manually
(A3851)	Authentication			_
HMAC-SHA2-256	Message	SW/FW Integrity	On Demand	Manually
(A3852)	Authentication			
HMAC-SHA2-256	Message	SW/FW Integrity	On Demand	Manually
(A3853)	Authentication			
HMAC-SHA2-256	Message	SW/FW Integrity	On Demand	Manually
(A3857)	Authentication			
HMAC-SHA2-256	Message	SW/FW Integrity	On Demand	Manually
(A3858)	Authentication			
HMAC-SHA2-512	Message	SW/FW Integrity	On Demand	Manually
(A3812)	Authentication			
HMAC-SHA2-512	Message	SW/FW Integrity	On Demand	Manually
(A3813)	Authentication			
HMAC-SHA2-512	Message	SW/FW Integrity	On Demand	Manually
(A3814)	Authentication			
HMAC-SHA2-512	Message	SW/FW Integrity	On Demand	Manually
(A3832)	Authentication			
HMAC-SHA2-512	Message	SW/FW Integrity	On Demand	Manually
(A3850)	Authentication			
HMAC-SHAZ-512	Message	SW/FW Integrity	On Demand	Manually
(A3851)	Auchentication		On Daman d	
	Message	SW/FW Integrity	On Demand	Manually
	Authentication		On Domand	Magually
	Message	SW/FW Integrity	On Demand	Manually
(ASOSO) DSA SiaVor	Signature	SW/EW/lotogrity	On Domand	Manually
(FIDS186-A) (A381A)	Verification	Sw/Fw mueghuy		Mandally
DSA SigVer	Signature	SW/FW/Integrity	On Demand	Manually
(FIPS186-4) (A3832)	Verification	Swyr w megney		Mandatty
RSA SigVer	Signature	SW/FW Integrity	On Demand	Manually
(FIPS186-4) (Δ3850)	Verification	Sw/r w meegney		
RSA SigVer	Signature	SW/FW Integrity	On Demand	Manually
(FIPS186-4) (Δ3851)	Verification	Swyr w micegnicy		
RSA SigVer	Signature	SW/FW Integrity	On Demand	Manually
(FIPS186-4) (A3852)	Verification	,		

Table 22: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-ECB (A3812)	КАТ	CAST	On Demand	Manually
AES-ECB (A3813)	КАТ	CAST	On Demand	Manually
AES-ECB (A3814)	КАТ	CAST	On Demand	Manually
AES-ECB (A3820)	КАТ	CAST	On Demand	Manually
AES-ECB (A3821)	КАТ	CAST	On Demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-ECB (A3822)	КАТ	CAST	On Demand	Manually
AES-ECB (A3824)	КАТ	CAST	On Demand	Manually
AES-ECB (A3825)	КАТ	CAST	On Demand	Manually
AES-ECB (A3829)	КАТ	CAST	On Demand	Manually
AES-ECB (A3830)	КАТ	CAST	On Demand	Manually
AES-ECB (A3831)	КАТ	CAST	On Demand	Manually
AES-ECB (A3832)	КАТ	CAST	On Demand	Manually
AES-ECB (A3833)	КАТ	CAST	On Demand	Manually
AES-ECB (A3834)	КАТ	CAST	On Demand	Manually
AES-ECB (A3840)	КАТ	CAST	On Demand	Manually
AES-ECB (A3841)	КАТ	CAST	On Demand	Manually
AES-ECB (A3842)	КАТ	CAST	On Demand	Manually
AES-ECB (A3843)	KAT	CAST	On Demand	Manually
AES-ECB (A3844)	КАТ	CAST	On Demand	Manually
AES-ECB (A3845)	KAT	CAST	On Demand	Manually
AFS-FCB (A3853)	KAT	CAST	On Demand	Manually
AES-ECB (A3854)	KAT	CAST	On Demand	Manually
AFS-FCB (A3855)	KAT	CAST	On Demand	Manually
AES-ECB (A3856)	KAT	CAST	On Demand	Manually
AES-ECB (A3857)	KAT	CAST	On Demand	Manually
AFS-FCB (A3812)	КАТ	CAST	On Demand	Manually
AFS-FCB (A3813)	KAT	CAST	On Demand	Manually
AFS-FCB (A3814)	ΚΔΤ	CAST	On Demand	Manually
Δ ES-ECB (Δ 3820)	κδτ	CAST	On Demand	Manually
$\Delta FS-FCB (\Delta 3821)$	κατ	CAST	On Demand	Manually
AES-ECB (A3822)	κατ	CAST	On Demand	Manually
AES-ECB (A3824)	κατ	CAST	On Demand	Manually
AES-ECB (A3825)	κατ	CAST	On Demand	Manually
AES-ECB (A3829)	KAT	CAST	On Demand	Manually
AES-ECB (A3830)	κατ	CAST	On Demand	Manually
AES ECB (A3831)	KAT	CAST	On Demand	Manually
AES-ECB (A3832)	KAT	CAST	On Demand	Manually
ALS-LCD (A3032)		CAST	On Demand	Manually
ALS-LCD (A3033)		CAST	On Demand	Manually
AES-ECD (A3834)		CAST	On Demand	Manually
AES-ECD (A3640)		CAST	On Demand	Manually
AES-ECD (A3641)		CAST	On Demand	Manually
AES-ECB (A3842)		CAST	On Demand	Manually
AES-ECB (A3843)		CAST	On Demand	Manually
		CAST	On Demand	Manually
		CAST	On Demand	Manually
AES-ECB (A3853)		CAST	On Demand	Manually
AES-ECB (A3854)	KAT	CAST	On Demand	Manually
AES-ECB (A3855)	KAI	CASI	On Demand	Manually
AES-ECB (A3856)	KAI	CASI	On Demand	Manually
ALS-ECB (A3857)	KAT	CAST	On Demand	Manually
AES-CBC (A3814)	KAT	CAST	On Demand	Manually
AES-CBC (A3822)	KAT	CAST	On Demand	Manually
AES-CBC (A3829)	KAT	CAST	On Demand	Manually
AES-CBC (A3832)	KAT	CAST	On Demand	Manually
AES-CBC (A3840)	KAT	CAST	On Demand	Manually
AES-CBC (A3843)	КАТ	CAST	On Demand	Manually
AES-CBC (A3853)	KAT	CAST	On Demand	Manually

AES-CBC (A3854) KAT CAST On Demand Manually AES-CBC (A3817) KAT CAST On Demand Manually AES-CBC (A3827) KAT CAST On Demand Manually AES-CBC (A3829) KAT CAST On Demand Manually AES-CBC (A3829) KAT CAST On Demand Manually AES-CBC (A3829) KAT CAST On Demand Manually AES-CBC (A3840) KAT CAST On Demand Manually AES-CBC (A3843) KAT CAST On Demand Manually AES-CBC (A3854) KAT CAST On Demand Manually AES-CBC (A3854) KAT CAST On Demand Manually AES-CBC (A3857) KAT CAST On Demand Manually AES-CBC (A3857) KAT CAST On Demand Manually AES-CBC (A3857) KAT CAST On Demand Manually (A3849) AT CAST On Demand Manua	Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-CBC (A3857) KAT CAST On Demand Manually AES-CBC (A3822) KAT CAST On Demand Manually AES-CBC (A3822) KAT CAST On Demand Manually AES-CBC (A3822) KAT CAST On Demand Manually AES-CBC (A3823) KAT CAST On Demand Manually AES-CBC (A3843) KAT CAST On Demand Manually AES-CBC (A3853) KAT CAST On Demand Manually AES-CBC (A3853) KAT CAST On Demand Manually AES-CBC (A3857) KAT CAST On Demand Manually AES-CBC (A3857) KAT CAST On Demand Manually AES-CBC (CS3 KAT CAST On Demand Manually AES-CBC (CS3 KAT CAST On Demand Manually AES-CBC-CS3 KAT CAST On Demand Manually (A3849) AES <cbc-cs3< td=""> KAT CAST On Demand<td>AES-CBC (A3854)</td><td>КАТ</td><td>CAST</td><td>On Demand</td><td>Manually</td></cbc-cs3<>	AES-CBC (A3854)	КАТ	CAST	On Demand	Manually
AES-CBC (A3814) KAT CAST On Demand Manually AES-CBC (A3822) KAT CAST On Demand Manually AES-CBC (A3822) KAT CAST On Demand Manually AES-CBC (A3822) KAT CAST On Demand Manually AES-CBC (A3840) KAT CAST On Demand Manually AES-CBC (A3840) KAT CAST On Demand Manually AES-CBC (A3853) KAT CAST On Demand Manually AES-CBC (A3854) KAT CAST On Demand Manually AES-CBC (A3857) KAT CAST On Demand Manually AES-CBC (A3857) KAT CAST On Demand Manually (A3819) AF CAST On Demand Manually (A3828) AF CAST On Demand Manually (A3838) AF CAST On Demand Manually (A3849) AF CAST On Demand Manually	AES-CBC (A3857)	КАТ	CAST	On Demand	Manually
AES-GEC (A3822) KAT CAST On Demand Manually AES-GEC (A3822) KAT CAST On Demand Manually AES-GE (A3842) KAT CAST On Demand Manually AES-GE (A3843) KAT CAST On Demand Manually AES-GE (A3843) KAT CAST On Demand Manually AES-GE (A3854) KAT CAST On Demand Manually AES-GE (A3854) KAT CAST On Demand Manually AES-GE (A3857) KAT CAST On Demand Manually AES-GEC-CS3 KAT CAST On Demand Manually AES-GEC-CS3 KAT CAST On Demand Manually (A3828) AES-GE-CCS3 KAT CAST On Demand Manually (A3824) AES-GE-CCS3 KAT CAST On Demand Manually (A3828) AES-GE-CCS3 KAT CAST On Demand Manually (A3824) AES-GE-CCS3	AES-CBC (A3814)	КАТ	CAST	On Demand	Manually
AES-GEC (A3829) KAT CAST On Demand Manually AES-GE (A3832) KAT CAST On Demand Manually AES-GE (A3840) KAT CAST On Demand Manually AES-GE (A3840) KAT CAST On Demand Manually AES-GE (A3840) KAT CAST On Demand Manually AES-GE (A3853) KAT CAST On Demand Manually AES-CEC (A3854) KAT CAST On Demand Manually AES-CEC (CS3 KAT CAST On Demand Manually (A3819) AES-GECCS3 KAT CAST On Demand Manually (A3849)	AES-CBC (A3822)	КАТ	CAST	On Demand	Manually
AES-GEC (A3832) KAT CAST On Demand Manually AES-CBC (A3840) KAT CAST On Demand Manually AES-CBC (A3843) KAT CAST On Demand Manually AES-CBC (A3843) KAT CAST On Demand Manually AES-CBC (A3854) KAT CAST On Demand Manually AES-CBC (A3857) KAT CAST On Demand Manually AES-CBC-CS3 KAT CAST On Demand Manually AES-CBC-CS3 KAT CAST On Demand Manually (A3389) AST CAST On Demand Manually (A3383) AST CAST On Demand Manually (A3384) AST CAST On Demand Manually (A3384) AST CAST On Demand Manually (A3384) AST CAST On Demand Manually (A3849) AST CAST On Demand Manually (A3849)	AES-CBC (A3829)	КАТ	CAST	On Demand	Manually
AES-CBC (A3840) KAT CAST On Demand Manually AES-CBC (A3843) KAT CAST On Demand Manually AES-CBC (A3853) KAT CAST On Demand Manually AES-CBC (A3853) KAT CAST On Demand Manually AES-CBC (A3850) KAT CAST On Demand Manually AES-CBC (C33 KAT CAST On Demand Manually AES-CBC-CS3 KAT CAST On Demand Manually (A3819) AES-CBC-CS3 KAT CAST On Demand Manually (A3849) AES-CBC-CS3 KAT CAST On Demand	AES-CBC (A3832)	КАТ	CAST	On Demand	Manually
AES-CBC (A3843) KAT CAST On Demand Manually AES-CBC (A3853) KAT CAST On Demand Manually AES-CBC (A3853) KAT CAST On Demand Manually AES-CBC (A3857) KAT CAST On Demand Manually AES-CBC (A3857) KAT CAST On Demand Manually AES-CBC-CS3 KAT CAST On Demand Manually (A3819) AES-CBC-CS3 KAT CAST On Demand Manually (A3828) AES-CBC-CS3 KAT CAST On Demand Manually (A3828) AES-CBC-CS3 KAT CAST On Demand Manually (A3849) AES-CBC-CS3 KAT CAST On Demand Manually (A3853) AES-CBC-CS3 KAT CAST On Demand Manually (A3849) AES-CBC-CS3 KAT CAST On Demand Manually (A3854) AES-CBC-CS3 KAT CAST On Demand Manually (A3853) AES-CBC-CS3 KAT CAST On	AES-CBC (A3840)	КАТ	CAST	On Demand	Manually
AES-CBC (A3853) KAT CAST On Demand Manually AES-CBC (A3854) KAT CAST On Demand Manually AES-CBC (A3857) KAT CAST On Demand Manually AES-CBC (A3857) KAT CAST On Demand Manually AES-CBC (CS3 KAT CAST On Demand Manually (A3819) AES-CBC-CS3 KAT CAST On Demand Manually (A3828) KAT CAST On Demand Manually (A3849) CAST On Demand Manually (A3849) AES-CBC-CS3 KAT CAST On Demand Manually <tr< td=""><td>AES-CBC (A3843)</td><td>КАТ</td><td>CAST</td><td>On Demand</td><td>Manually</td></tr<>	AES-CBC (A3843)	КАТ	CAST	On Demand	Manually
AES-CBC (A3854) KAT CAST On Demand Manually AES-CBC (A3857) KAT CAST On Demand Manually AES-CBC-CS3 KAT CAST On Demand Manually (A3819) AES-CBC-CS3 KAT CAST On Demand Manually (A3828) CAST On Demand Manually Manually (A3828) CAST On Demand Manually (A3849) CAST On Demand Manually (A3854) CAST On Demand Manually (A3853) KAT CAST On Demand Manually (A3854) KAT CAST On Demand </td <td>AES-CBC (A3853)</td> <td>КАТ</td> <td>CAST</td> <td>On Demand</td> <td>Manually</td>	AES-CBC (A3853)	КАТ	CAST	On Demand	Manually
AES-CBC (A3857) KAT CAST On Demand Manually AES-CBC-CS3 KAT CAST On Demand Manually (A3819) AES-CBC-CS3 KAT CAST On Demand Manually AES-CBC-CS3 KAT CAST On Demand Manually (A3828) AES-CBC-CS3 KAT CAST On Demand Manually (A3838) AES-CBC-CS3 KAT CAST On Demand Manually (A3839) AES-CBC-CS3 KAT CAST On Demand Manually (A3853) AES-CBC-CS3 KAT CAST On Demand Manually (A3853) AES-CBC-CS3 KAT CAST On Demand Manually (A3853) AES-CBC-CS3 KAT CAST On Demand Manually (A3828) AES-CBC-CS3	AES-CBC (A3854)	КАТ	CAST	On Demand	Manually
AES-CBC-CS3 KAT CAST On Demand Manually (A3819) AES-CBC-CS3 KAT CAST On Demand Manually (A3828) AES-CBC-CS3 KAT CAST On Demand Manually (A3838) AES-CBC-CS3 KAT CAST On Demand Manually (A3849) AES-CBC-CS3 KAT CAST On Demand Manually (A3849) AES-CBC-CS3 KAT CAST On Demand Manually (A3853) AES-CBC-CS3 KAT CAST On Demand Manually (A3849) AES-CBC-CS3 KAT CAST On Demand Manually (A3849) AES-CBC-CS3 KAT CAST On Demand Manually (A3828) AES-CBC-CS3 KAT CAST On Demand Manually (A3828) AES-CBC-CS3 KAT CAST On Demand Manually (A3838) AES-CBC-CS3 KAT CAST On Demand Manually (A3849) AES-CBC-CS3 KAT CAST On Demand Manually <	AES-CBC (A3857)	КАТ	CAST	On Demand	Manually
(A3819)CASTOn DemandManuallyAES-CBC-CS3KATCASTOn DemandManually(A3828)AES-CBC-CS3KATCASTOn DemandManually(A3849)AES-CBC-CS3KATCASTOn DemandManually(A3849)AES-CBC-CS3KATCASTOn DemandManually(A3853)AES-CBC-CS3KATCASTOn DemandManually(A3853)AES-CBC-CS3KATCASTOn DemandManually(A3854)AES-CBC-CS3KATCASTOn DemandManually(A3828)AES-CBC-CS3KATCASTOn DemandManually(A3828)AES-CBC-CS3KATCASTOn DemandManually(A3828)AES-CBC-CS3KATCASTOn DemandManually(A3849)AES-CBC-CS3KATCASTOn DemandManually(A3849)AES-CBC-CS3KATCASTOn DemandManually(A3853)AES-CBC-CS3KATCASTOn DemandManually(A3854)AES-CFB128KATCASTOn DemandManually(A3854)AES-CFB128KATCASTOn DemandManually(A3826)AES-CFB128KATCASTOn DemandManually(A3826)AES-CFB128KATCASTOn DemandManually(A3826)AES-CFB128KATCASTOn DemandManually(A3836)AES-CFB128KATCASTOn DemandManually </td <td>AES-CBC-CS3</td> <td>KAT</td> <td>CAST</td> <td>On Demand</td> <td>Manually</td>	AES-CBC-CS3	KAT	CAST	On Demand	Manually
AES-CBC-CS3 KAT CAST On Demand Manually (A3828) KAT CAST On Demand Manually (A3838) KAT CAST On Demand Manually (A3849) CAST On Demand Manually (A3853) KAT CAST On Demand Manually (A3854) CAST On Demand Manually Manually (A3854) KAT CAST On Demand Manually (A3859) KAT CAST On Demand Manually (A3828) KAT CAST On Demand Manually (A3828) KAT CAST On Demand Manually (A3828) KAT CAST On Demand Manually (A3849) AT CAST On Demand Manually (A3849) AT CAST On Demand Manually (A38	(A3819)				
(A3828)CASTOn DemandManuallyAES-CBC-CS3KATCASTOn DemandManually(A3838)AES-CBC-CS3KATCASTOn DemandManually(A3849)AES-CBC-CS3KATCASTOn DemandManually(A3853)AES-CBC-CS3KATCASTOn DemandManually(A3854)AES-CBC-CS3KATCASTOn DemandManually(A3854)AES-CBC-CS3KATCASTOn DemandManually(A3828)AES-CBC-CS3KATCASTOn DemandManually(A3839)AES-CBC-CS3KATCASTOn DemandManually(A3839)AES-CBC-CS3KATCASTOn DemandManually(A3838)AES-CBC-CS3KATCASTOn DemandManually(A3839)AES-CBC-CS3KATCASTOn DemandManually(A3834)AES-CBC-CS3KATCASTOn DemandManually(A3837)AES-CBC-CS3KATCASTOn DemandManually(A3837)AES-CFB128KATCASTOn DemandManually(A3836)AES-CFB128KATCASTOn DemandManually(A3836)AES-CFB128KATCASTOn DemandManually(A3837)AES-CFB128KATCASTOn DemandManually(A3837)AES-CFB128KATCASTOn DemandManually(A3837)AES-CFB128KATCASTOn DemandManually </td <td>AES-CBC-CS3</td> <td>КАТ</td> <td>CAST</td> <td>On Demand</td> <td>Manually</td>	AES-CBC-CS3	КАТ	CAST	On Demand	Manually
AES-CBC-CS3 (A3849)KATCASTOn DemandManuallyAES-CBC-CS3 (A3849)KATCASTOn DemandManuallyAES-CBC-CS3 (A3853)KATCASTOn DemandManuallyAES-CBC-CS3 (A3853)KATCASTOn DemandManuallyAES-CBC-CS3 (A3819)KATCASTOn DemandManuallyAES-CBC-CS3 (A3819)KATCASTOn DemandManuallyAES-CBC-CS3 (A3819)KATCASTOn DemandManuallyAES-CBC-CS3 (A3838)KATCASTOn DemandManuallyAES-CBC-CS3 (A3849)KATCASTOn DemandManually(A3849)ASOn DemandManually(A3849)ASCASTOn DemandManually(A3849)ASCASTOn DemandManually(A3843)CASTOn DemandManually(A3844)CASTOn DemandManually(A3843)CASTOn DemandManually(A3844)CASTOn DemandManually(A3847)CASTOn DemandManually(A3847)CASTOn DemandManually(A3847)CASTOn DemandManually(A3847)CASTOn DemandManually(A3847)CASTOn DemandManually(A3847)CASTOn DemandManually(A3847)CASTOn DemandManually(A3847)CASTOn DemandManually<	(A3828)				· · · · · · · · · · · · · · · · · · ·
(A3838)CASTCASTOn DemandManuallyAES-CBC-CS3KATCASTOn DemandManually(A3849)AES-CBC-CS3KATCASTOn DemandManually(A3853)AES-CBC-CS3KATCASTOn DemandManually(A3854)AES-CBC-CS3KATCASTOn DemandManually(A3819)AES-CBC-CS3KATCASTOn DemandManually(A3828)AES-CBC-CS3KATCASTOn DemandManually(A3838)AES-CBC-CS3KATCASTOn DemandManually(A3838)AES-CBC-CS3KATCASTOn DemandManually(A3849)AES-CBC-CS3KATCASTOn DemandManually(A3854)AES-CBC-CS3KATCASTOn DemandManually(A3854)AES-CBC-CS3KATCASTOn DemandManually(A3854)AES-CPB128KATCASTOn DemandManually(A3854)AES-CPB128KATCASTOn DemandManually(A3847)AES-CPB128KATCASTOn DemandManually(A3847)AES-CPB128KATCASTOn DemandManually(A3847)AES-CPB128KATCASTOn DemandManually(A3854)AES-CPB128KATCASTOn DemandManually(A3854)AES-CPB128KATCASTOn DemandManually(A3856)AES-CPB128KATCASTOn Demand <td< td=""><td>AES-CBC-CS3</td><td>КАТ</td><td>CAST</td><td>On Demand</td><td>Manually</td></td<>	AES-CBC-CS3	КАТ	CAST	On Demand	Manually
AES-CBC-CS3KATCASTOn DemandManually(A3849)AES-CBC-CS3KATCASTOn DemandManually(A3853)AES-CBC-CS3KATCASTOn DemandManually(A3854)AES-CBC-CS3KATCASTOn DemandManually(A3854)AES-CBC-CS3KATCASTOn DemandManually(A3859)AES-CBC-CS3KATCASTOn DemandManually(A3828)AES-CBC-CS3KATCASTOn DemandManually(A3838)AES-CBC-CS3KATCASTOn DemandManually(A3849)AES-CBC-CS3KATCASTOn DemandManually(A3849)AES-CBC-CS3KATCASTOn DemandManually(A3849)AES-CBC-CS3KATCASTOn DemandManually(A3843)AES-CBC-CS3KATCASTOn DemandManually(A3843)AES-CBC-CS3KATCASTOn DemandManually(A3847)AES-CFB128KATCASTOn DemandManually(A3847)AES-CFB128KATCASTOn DemandManually(A3847)AES-CFB128KATCASTOn DemandManually(A3847)AES-CFB128KATCASTOn DemandManually(A3847)AES-CFB128KATCASTOn DemandManually(A3847)AES-CFB128KATCASTOn DemandManually(A3847)AES-CFB128KATCAST<	(A3838)				, , , , , , , , , , , , , , , , , , ,
(A3849)CASTOn DemandManuallyAES-CBC-CS3KATCASTOn DemandManually(A3853)AES-CBC-CS3KATCASTOn DemandManually(A3819)AES-CBC-CS3KATCASTOn DemandManually(A3819)AES-CBC-CS3KATCASTOn DemandManually(A3838)AES-CBC-CS3KATCASTOn DemandManually(A3838)AES-CBC-CS3KATCASTOn DemandManually(A3838)AES-CBC-CS3KATCASTOn DemandManually(A3839)AES-CBC-CS3KATCASTOn DemandManually(A3834)AES-CBC-CS3KATCASTOn DemandManually(A3854)AES-CFB128KATCASTOn DemandManually(A3847)AES-CFB128KATCASTOn DemandManually(A3847)AES-CFB128KATCASTOn DemandManually(A3847)AES-CFB128KATCASTOn DemandManually(A3847)AES-CFB128KATCASTOn DemandManually(A3847)AES-CFB128KATCASTOn DemandManually(A3844)AES-CFB128KATCASTOn DemandManually(A3847)AES-CFB128KATCASTOn DemandManually(A3843)AES-CFB128KATCASTOn DemandManually(A3847)AES-CFB128KATCASTOn DemandManually<	AES-CBC-CS3	КАТ	CAST	On Demand	Manually
AES-CBC-CS3 (A3853)KATCASTOn DemandManuallyAES-CBC-CS3 (A3854)KATCASTOn DemandManually(A3854)AES-CBC-CS3KATCASTOn DemandManually(A3819)AES-CBC-CS3KATCASTOn DemandManually(A3828)AES-CBC-CS3KATCASTOn DemandManually(A3838)AES-CBC-CS3KATCASTOn DemandManually(A3838)AES-CBC-CS3KATCASTOn DemandManually(A3849)AES-CBC-CS3KATCASTOn DemandManually(A3853)AES-CBC-CS3KATCASTOn DemandManually(A3854)AES-CBC-CS3KATCASTOn DemandManually(A3854)AES-CFB128KATCASTOn DemandManually(A3854)AES-CFB128KATCASTOn DemandManually(A3877)AES-CFB128KATCASTOn DemandManually(A3847)AES-CFB128KATCASTOn DemandManually(A3847)AES-CFB128KATCASTOn DemandManually(A3847)AES-CFB128KATCASTOn DemandManually(A3847)AES-CFB128KATCASTOn DemandManually(A3847)AES-CFB128KATCASTOn DemandManually(A3847)AES-CFB128KATCASTOn DemandManually(A3847)AES-CFB128KATCAST<	(A3849)				
(A3853)CASTOn DemandManuallyAES-CBC-CS3KATCASTOn DemandManually(A3854)AES-CBC-CS3KATCASTOn DemandManually(A3819)AES-CBC-CS3KATCASTOn DemandManually(A3828)AES-CBC-CS3KATCASTOn DemandManually(A3838)AES-CBC-CS3KATCASTOn DemandManually(A3839)AES-CBC-CS3KATCASTOn DemandManually(A3849)AES-CBC-CS3KATCASTOn DemandManually(A3853)AES-CBC-CS3KATCASTOn DemandManually(A3853)AES-CBC-CS3KATCASTOn DemandManually(A3853)AES-CFB128KATCASTOn DemandManually(A3817)AES-CFB128KATCASTOn DemandManually(A3826)AES-CFB128KATCASTOn DemandManually(A3847)AES-CFB128KATCASTOn DemandManually(A3847)AES-CFB128KATCASTOn DemandManually(A3847)AES-CFB128KATCASTOn DemandManually(A3846)AES-CFB128KATCASTOn DemandManually(A3863)AES-CFB128KATCASTOn DemandManually(A3863)AES-CFB128KATCASTOn DemandManually(A3863)AES-CFB128KATCASTOn DemandManually<	AES-CBC-CS3	КАТ	CAST	On Demand	Manually
AES-CBC-CS3 (A3854)KATCASTOn DemandManuallyAES-CBC-CS3 (A3819)KATCASTOn DemandManuallyAES-CBC-CS3 (A3828)KATCASTOn DemandManuallyAES-CBC-CS3 (A3889)KATCASTOn DemandManuallyAES-CBC-CS3 (A3849)KATCASTOn DemandManuallyAES-CBC-CS3 (A3849)KATCASTOn DemandManuallyAES-CBC-CS3 (A3853)KATCASTOn DemandManually(A3849)AES-CBC-CS3 (A3854)KATCASTOn DemandManually(A3854)AES-CBC-CS3 (A3854)KATCASTOn DemandManually(A3854)KATCASTOn DemandManually(A3847)KATCASTOn DemandManually(A3847)KATCASTOn DemandManually(A3854)KATCASTOn DemandManually(A3847)KATCASTOn DemandManually(A3847)KATCASTOn DemandManually(A3847)KATCASTOn DemandManually(A3847)KATCASTOn DemandManually(A3847)KATCASTOn DemandManually(A3845)KATCASTOn DemandManually(A3845)KATCASTOn DemandManually(A3847)KATCASTOn DemandManually(A3845)KATCASTOn DemandManually </td <td>(A3853)</td> <td></td> <td></td> <td></td> <td>, , , , , , , , , , , , , , , , , , ,</td>	(A3853)				, , , , , , , , , , , , , , , , , , ,
(A3854)CASTOn DemandManually(A3819)AES-CBC-CS3KATCASTOn DemandManually(A3828)AES-CBC-CS3KATCASTOn DemandManually(A3838)AES-CBC-CS3KATCASTOn DemandManually(A3838)AES-CBC-CS3KATCASTOn DemandManually(A3849)AES-CBC-CS3KATCASTOn DemandManually(A3853)AES-CBC-CS3KATCASTOn DemandManually(A3854)AES-CBC-CS3KATCASTOn DemandManually(A3854)AES-CFB128KATCASTOn DemandManually(A3826)AES-CFB128KATCASTOn DemandManually(A3836)AES-CFB128KATCASTOn DemandManually(A3847)AES-CFB128KATCASTOn DemandManually(A3847)AES-CFB128KATCASTOn DemandManually(A3847)AES-CFB128KATCASTOn DemandManually(A3847)AES-CFB128KATCASTOn DemandManually(A3847)AES-CFB128KATCASTOn DemandManually(A3847)AES-CFB128KATCASTOn DemandManually(A3847)AES-CFB128KATCASTOn DemandManually(A3847)AES-CFB128KATCASTOn DemandManually(A3856)AES-CFB128KATCASTOn Demand	AES-CBC-CS3	КАТ	CAST	On Demand	Manually
AES-CBC-CS3 (A3819)KATCASTOn DemandManuallyAES-CBC-CS3 (A3828)KATCASTOn DemandManuallyAES-CBC-CS3 (A3838)KATCASTOn DemandManuallyAES-CBC-CS3 (A3849)KATCASTOn DemandManuallyAES-CBC-CS3 (A3849)KATCASTOn DemandManuallyAES-CBC-CS3 (A3853)KATCASTOn DemandManually(A3849)AES-CBC-CS3KATCASTOn DemandManually(A3853)KATCASTOn DemandManually(A3854)AES-CFB128KATCASTOn DemandManually(A386)AES-CFB128KATCASTOn DemandManually(A3836)AES-CFB128KATCASTOn DemandManually(A3847)AES-CFB128KATCASTOn DemandManually(A3847)AES-CFB128KATCASTOn DemandManually(A3847)AES-CFB128KATCASTOn DemandManually(A3847)AES-CFB128KATCASTOn DemandManually(A3847)AES-CFB128KATCASTOn DemandManually(A3854)AES-CFB128KATCASTOn DemandManually(A3856)AES-CFB128KATCASTOn DemandManually(A386)AES-CFB128KATCASTOn DemandManually(A3836)AES-CFB128KATCASTOn DemandManually<	(A3854)				
(A3819)CASTOn DemandManuallyAES-CBC-CS3KATCASTOn DemandManually(A3828)AES-CBC-CS3KATCASTOn DemandManually(A3838)AES-CBC-CS3KATCASTOn DemandManually(A3849)AES-CBC-CS3KATCASTOn DemandManually(A3853)AES-CBC-CS3KATCASTOn DemandManually(A3854)AES-CFB128KATCASTOn DemandManually(A3817)AES-CFB128KATCASTOn DemandManually(A3826)AES-CFB128KATCASTOn DemandManually(A3847)AES-CFB128KATCASTOn DemandManually	AES-CBC-CS3	КАТ	CAST	On Demand	Manually
AES-CBC-CS3 (A3828)KATCASTOn DemandManuallyAES-CBC-CS3 (A3838)KATCASTOn DemandManuallyAES-CBC-CS3 (A3849)KATCASTOn DemandManuallyAES-CBC-CS3 (A3853)KATCASTOn DemandManuallyAES-CBC-CS3 (A3853)KATCASTOn DemandManuallyAES-CBC-CS3 (A3853)KATCASTOn DemandManuallyAES-CBC-CS3 (A3854)KATCASTOn DemandManuallyAES-CFB128 (A3826)KATCASTOn DemandManuallyAES-CFB128 (A3826)KATCASTOn DemandManuallyAES-CFB128 (A3847)KATCASTOn DemandManually(A3847)CASTOn DemandManuallyAES-CFB128 (A3847)KATCASTOn DemandManually(A3847)CASTOn DemandManuallyAES-CFB128 (A3847)KATCASTOn DemandManually(A3847)CASTOn DemandManually(A3847)CASTOn DemandManually(A3847)CASTOn DemandManually(A3847)CASTOn DemandManually(A3847)CASTOn DemandManually(A3847)CASTOn DemandManually(A3847)CASTOn DemandManually(A3847)CASTOn DemandManually(A3	(A3819)				-
(A3828)KATCASTOn DemandManually(A3838)KATCASTOn DemandManually(A3838)KATCASTOn DemandManually(A3849)AES-CBC-CS3KATCASTOn DemandManually(A3853)KATCASTOn DemandManually(A3854)KATCASTOn DemandManually(A3854)KATCASTOn DemandManuallyAES-CFB128KATCASTOn DemandManually(A3817)AES-CFB128KATCASTOn DemandManually(A3847)AES-CFB128KATCASTOn DemandM	AES-CBC-CS3	КАТ	CAST	On Demand	Manually
AES-CBC-CS3 (A3838)KATCASTOn DemandManuallyAES-CBC-CS3 (A3849)KATCASTOn DemandManuallyAES-CBC-CS3 (A3853)KATCASTOn DemandManually(A3849)AES-CBC-CS3 (A3853)KATCASTOn DemandManually(A3854)AES-CFB128 (A3854)KATCASTOn DemandManually(A3854)AES-CFB128 (A3817)KATCASTOn DemandManually(A3854)AES-CFB128 (A386)KATCASTOn DemandManually(A386)AES-CFB128 (A386)KATCASTOn DemandManually(A386)CASTOn DemandManually(A3864)CASTOn DemandManually(A3864)CASTOn DemandManually(A3864)CASTOn DemandManually(A3864)CASTOn DemandManually(A3877)CASTOn DemandManually(A3877)CASTOn DemandManually(A3877)CASTOn DemandManually(A3877)CASTOn DemandManually(A3876)CASTOn DemandManually(A3836)CASTOn DemandManually(A3836)CASTOn DemandManually(A3836)CASTOn DemandManually(A3836)CASTOn DemandManually(A3836)CASTOn DemandManually(A3836)CASTOn Demand <td< td=""><td>(A3828)</td><td></td><td></td><td></td><td>-</td></td<>	(A3828)				-
(A3838)KATCASTOn DemandManually(A3849)AES-CBC-CS3KATCASTOn DemandManually(A3853)AES-CBC-CS3KATCASTOn DemandManually(A3854)AES-CFB128KATCASTOn DemandManually(A3854)AES-CFB128KATCASTOn DemandManually(A3817)AES-CFB128KATCASTOn DemandManually(A3826)AES-CFB128KATCASTOn DemandManually(A3836)AES-CFB128KATCASTOn DemandManually(A3847)AES-CFB128KATCASTOn DemandManually(A3846)AES-CFB128KATCASTOn Demand </td <td>AES-CBC-CS3</td> <td>КАТ</td> <td>CAST</td> <td>On Demand</td> <td>Manually</td>	AES-CBC-CS3	КАТ	CAST	On Demand	Manually
AES-CBC-CS3 (A3849)KATCASTOn DemandManuallyAES-CBC-CS3 (A3853)KATCASTOn DemandManually(A3853)AES-CBC-CS3KATCASTOn DemandManually(A3854)AES-CFB128KATCASTOn DemandManually(A3817)AES-CFB128KATCASTOn DemandManually(A3826)AES-CFB128KATCASTOn DemandManually(A3836)AES-CFB128KATCASTOn DemandManually(A3836)AES-CFB128KATCASTOn DemandManually(A3847)CASTOn DemandManuallyAES-CFB128KATCASTOn DemandManually(A3847)CASTOn DemandManuallyAES-CFB128KATCASTOn DemandManually(A3847)CASTOn DemandManuallyAES-CFB128KATCASTOn DemandManually(A3854)CASTOn DemandManually(A3854)CASTOn DemandManually(A3854)CASTOn DemandManually(A3854)CASTOn DemandManually(A3854)CASTOn DemandManually(A3854)CASTOn DemandManually(A3854)CASTOn DemandManually(A3826)CASTOn DemandManually(A3826)CASTOn DemandManually(A3826)CASTOn DemandManuall	(A3838)				
(A3849)CASTOn DemandManuallyAES-CBC-CS3 (A3853)KATCASTOn DemandManuallyAES-CBC-CS3 (A3854)KATCASTOn DemandManuallyAES-CFB128 (A3817)KATCASTOn DemandManuallyAES-CFB128 (A3826)KATCASTOn DemandManuallyAES-CFB128 (A3836)KATCASTOn DemandManuallyAES-CFB128 (A3847)KATCASTOn DemandManuallyAES-CFB128 (A3847)KATCASTOn DemandManuallyAES-CFB128 (A3847)KATCASTOn DemandManuallyAES-CFB128 (A3847)KATCASTOn DemandManuallyAES-CFB128 (A3854)KATCASTOn DemandManuallyAES-CFB128 (A3854)KATCASTOn DemandManuallyAES-CFB128 (A3854)KATCASTOn DemandManuallyAES-CFB128 (A3826)KATCASTOn DemandManuallyAES-CFB128 (A3836)KATCASTOn DemandManuallyAES-CFB128 (A3836)KATCASTOn DemandManuallyAES-CFB128 (A2847)KATCASTOn DemandManuallyAES-CFB128 (A2826)KATCASTOn DemandManuallyAES-CFB128 (A2827)KATCASTOn DemandManuallyAES-CFB128 (A2827)KATCASTOn DemandManuallyAES-CFB128 (A2827)KATCAST <td< td=""><td>AES-CBC-CS3</td><td>КАТ</td><td>CAST</td><td>On Demand</td><td>Manually</td></td<>	AES-CBC-CS3	КАТ	CAST	On Demand	Manually
AES-CBC-CS3 (A3853)KATCASTOn DemandManuallyAES-CFC-CS3 (A3854)KATCASTOn DemandManuallyAES-CFB128 (A3817)KATCASTOn DemandManuallyAES-CFB128 (A3826)KATCASTOn DemandManuallyAES-CFB128 (A3836)KATCASTOn DemandManuallyAES-CFB128 (A3836)KATCASTOn DemandManuallyAES-CFB128 (A3847)KATCASTOn DemandManuallyAES-CFB128 (A3847)KATCASTOn DemandManuallyAES-CFB128 (A3847)KATCASTOn DemandManuallyAES-CFB128 (A3854)KATCASTOn DemandManuallyAES-CFB128 (A3854)KATCASTOn DemandManuallyAES-CFB128 (A3826)KATCASTOn DemandManuallyAES-CFB128 (A3836)KATCASTOn DemandManuallyAES-CFB128 (A3836)KATCASTOn DemandManuallyAES-CFB128 (A3836)KATCASTOn DemandManuallyAES-CFB128 (A3836)KATCASTOn DemandManuallyAES-CFB128 (A3836)KATCASTOn DemandManuallyAES-CFB128 (A3836)KATCASTOn DemandManuallyAES-CFB128 (A3836)KATCASTOn DemandManuallyAES-CFB128 (A3836)KATCASTOn DemandManuallyAES-CFB128 (A3836)<	(A3849)				
(A3853)KATCASTOn DemandManuallyAES-CRS128KATCASTOn DemandManually(A387)AES-CFB128KATCASTOn DemandManually(A3826)AES-CFB128KATCASTOn DemandManually(A3836)AES-CFB128KATCASTOn DemandManually(A3836)AES-CFB128KATCASTOn DemandManually(A3847)AES-CFB128KATCASTOn DemandManually(A3847)AES-CFB128KATCASTOn DemandManually(A3854)AES-CFB128KATCASTOn DemandManually(A3854)AES-CFB128KATCASTOn DemandManually(A3854)AES-CFB128KATCASTOn DemandManually(A3836)AES-CFB128KATCASTOn DemandManually(A3836)AES-CFB128KATCASTOn DemandManually(A3836)AES-CFB128KATCASTOn DemandManually(A3836)AES-CFB128KATCASTOn DemandManually(A3836)AES-CFB128KATCASTOn DemandManually(A3836)AES-CFB128KATCASTOn DemandManually(A3836)AES-CFB128KATCASTOn DemandManually	AES-CBC-CS3	КАТ	CAST	On Demand	Manually
AES-CBC-CS3 (A3854)KATCASTOn DemandManuallyAES-CFB128 (A3817)KATCASTOn DemandManuallyAES-CFB128 (A3826)KATCASTOn DemandManuallyAES-CFB128 (A3836)KATCASTOn DemandManuallyAES-CFB128 (A3847)KATCASTOn DemandManuallyAES-CFB128 (A3847)KATCASTOn DemandManuallyAES-CFB128 (A3847)KATCASTOn DemandManuallyAES-CFB128 (A3854)KATCASTOn DemandManuallyAES-CFB128 (A3854)KATCASTOn DemandManuallyAES-CFB128 (A3817)KATCASTOn DemandManuallyAES-CFB128 (A3836)KATCASTOn DemandManuallyAES-CFB128 (A3836)KATCASTOn DemandManuallyAES-CFB128 (A3836)KATCASTOn DemandManuallyAES-CFB128 (A3836)KATCASTOn DemandManuallyAES-CFB128 (A3836)KATCASTOn DemandManuallyAES-CFB128 (A3847)KATCASTOn DemandManuallyAES-CFB128 (A3836)KATCASTOn DemandManuallyAES-CFB128 (A3847)KATCASTOn DemandManuallyAES-CFB128 (A3847)KATCASTOn DemandManuallyAES-CFB128 (A3847)KATCASTOn DemandManuallyAES-CFB128 (A3847) <t< td=""><td>(A3853)</td><td></td><td></td><td></td><td></td></t<>	(A3853)				
(A3854)KATCASTOn DemandManuallyAES-CFB128KATCASTOn DemandManually(A3826)KATCASTOn DemandManuallyAES-CFB128KATCASTOn DemandManually(A3836)AES-CFB128KATCASTOn DemandManually(A3847)AES-CFB128KATCASTOn DemandManually(A3847)AES-CFB128KATCASTOn DemandManually(A3847)AES-CFB128KATCASTOn DemandManually(A3854)AES-CFB128KATCASTOn DemandManually(A3854)AES-CFB128KATCASTOn DemandManually(A386)AES-CFB128KATCASTOn DemandManually(A3836)AES-CFB128KATCASTOn DemandManually(A3836)AES-CFB128KATCASTOn DemandManually(A3836)AES-CFB128KATCASTOn DemandManually	AES-CBC-CS3	КАТ	CAST	On Demand	Manually
AES-CFB128 (A3817)KATCASTOn DemandManually (A3826)AES-CFB128 (A3836)KATCASTOn DemandManually (A3836)AES-CFB128 (A3847)KATCASTOn DemandManually (Manually)AES-CFB128 (A3847)KATCASTOn DemandManually (Manually)AES-CFB128 (A3847)KATCASTOn DemandManually (Manually)AES-CFB128 (A3854)KATCASTOn DemandManually (Manually)AES-CFB128 (A3854)KATCASTOn DemandManually (Manually)AES-CFB128 (A386)KATCASTOn DemandManually (Manually)AES-CFB128 (A3836)KATCASTOn DemandManually (Manually)AES-CFB128 (A3836)KATCASTOn DemandManually (Manually)AES-CFB128 (A3836)KATCASTOn DemandManually (Manually)AES-CFB128 (A3847)KATCASTOn DemandManually	(A3854)				
(A3817)KATCASTOn DemandManually(A3826)KATCASTOn DemandManually(A3836)KATCASTOn DemandManually(A3847)KATCASTOn DemandManuallyAES-CFB128KATCASTOn DemandManually(A3847)AES-CFB128KATCASTOn DemandManually(A3847)AES-CFB128KATCASTOn DemandManually(A3854)AES-CFB128KATCASTOn DemandManually(A3857)AES-CFB128KATCASTOn DemandManually(A3826)KATCASTOn DemandManually(A3836)KATCASTOn DemandManually(A3836)KATCASTOn DemandManually(A3847)KATCASTOn DemandManually	AES-CFB128	КАТ	CAST	On Demand	Manually
AES-CFB128KATCASTOn DemandManually(A3826)AES-CFB128KATCASTOn DemandManually(A3836)AES-CFB128KATCASTOn DemandManually(A3847)AES-CFB128KATCASTOn DemandManually(A3854)AES-CFB128KATCASTOn DemandManually(A3854)AES-CFB128KATCASTOn DemandManually(A3857)AES-CFB128KATCASTOn DemandManually(A3817)AES-CFB128KATCASTOn DemandManually(A3826)AES-CFB128KATCASTOn DemandManually(A3836)AES-CFB128KATCASTOn DemandManually(A3836)AES-CFB128KATCASTOn DemandManually(A2847)KATCASTOn DemandManually	(A3817)				
(A3826)KATCASTOn DemandManually(A3836)AES-CFB128KATCASTOn DemandManually(A3847)AES-CFB128KATCASTOn DemandManually(A3854)AES-CFB128KATCASTOn DemandManually(A3817)AES-CFB128KATCASTOn DemandManually(A3817)AES-CFB128KATCASTOn DemandManually(A3817)AES-CFB128KATCASTOn DemandManually(A3826)AES-CFB128KATCASTOn DemandManually(A3836)AES-CFB128KATCASTOn DemandManually(A3836)AES-CFB128KATCASTOn DemandManually	AES-CFB128	КАТ	CAST	On Demand	Manually
AES-CFB128 (A3836)KATCASTOn DemandManuallyAES-CFB128 (A3847)KATCASTOn DemandManuallyAES-CFB128 (A3854)KATCASTOn DemandManuallyAES-CFB128 (A3817)KATCASTOn DemandManuallyAES-CFB128 (A3817)KATCASTOn DemandManuallyAES-CFB128 (A3817)KATCASTOn DemandManuallyAES-CFB128 (A3826)KATCASTOn DemandManuallyAES-CFB128 (A3836)KATCASTOn DemandManuallyAES-CFB128 (A3836)KATCASTOn DemandManuallyAES-CFB128 (A3836)KATCASTOn DemandManually	(A3826)				
(A3836)KATCASTOn DemandManuallyAES-CFB128KATCASTOn DemandManually(A3854)KATCASTOn DemandManuallyAES-CFB128KATCASTOn DemandManually(A3817)AES-CFB128KATCASTOn DemandManually(A3826)KATCASTOn DemandManuallyAES-CFB128KATCASTOn DemandManually(A3836)KATCASTOn DemandManuallyAES-CFB128KATCASTOn DemandManually(A3836)KATCASTOn DemandManually	AES-CFB128	КАТ	CAST	On Demand	Manually
AES-CFB128 (A3847)KATCASTOn DemandManuallyAES-CFB128 (A3854)KATCASTOn DemandManuallyAES-CFB128 (A3817)KATCASTOn DemandManuallyAES-CFB128 (A3826)KATCASTOn DemandManuallyAES-CFB128 (A3826)KATCASTOn DemandManuallyAES-CFB128 (A3836)KATCASTOn DemandManuallyAES-CFB128 (A3836)KATCASTOn DemandManuallyAES-CFB128 (A3836)KATCASTOn DemandManuallyAES-CFB128 (A3836)KATCASTOn DemandManually	(A3836)	1/A T			
(A3847)KATCASTOn DemandManually(A3854)AES-CFB128KATCASTOn DemandManually(A3817)AES-CFB128KATCASTOn DemandManually(A3826)AES-CFB128KATCASTOn DemandManually(A3836)AES-CFB128KATCASTOn DemandManually(A3836)AES-CFB128KATCASTOn DemandManually(A3836)AES-CFB128KATCASTOn DemandManually	AES-CFB128	KAT	CASI	On Demand	Manually
AES-CFB128KATCASTOn DemandManually(A3854)AES-CFB128KATCASTOn DemandManually(A3817)AES-CFB128KATCASTOn DemandManually(A3826)AES-CFB128KATCASTOn DemandManually(A3836)AES-CFB128KATCASTOn DemandManually(A3836)AES-CFB128KATCASTOn DemandManually(A2847)CASTOn DemandManually	(A3847)				
(A3854)KATCASTOn DemandManually(A3817)AES-CFB128KATCASTOn DemandManually(A3826)AES-CFB128KATCASTOn DemandManually(A3836)AES-CFB128KATCASTOn DemandManually(A3836)AES-CFB128KATCASTOn DemandManually	AES-CFB128	KAI	CASI	On Demand	Manually
AES-CFB128 (A3817)KATCASTOn DemandManuallyAES-CFB128 (A3826)KATCASTOn DemandManuallyAES-CFB128 (A3836)KATCASTOn DemandManuallyAES-CFB128 (A3836)KATCASTOn DemandManuallyAES-CFB128 (A3836)KATCASTOn DemandManually	(A3854)				
(A3817)CASTOn DemandManuallyAES-CFB128 (A3826)KATCASTOn DemandManuallyAES-CFB128 (A3836)KATCASTOn DemandManuallyAES-CFB128 (A3836)KATCASTOn DemandManually	AES-CFB128	КАТ	CAST	On Demand	Manually
AES-CFB128KATCASTOn DemandManually(A3826)AES-CFB128KATCASTOn DemandManually(A3836)AES-CFB128KATCASTOn DemandManually(A2847)CASTOn DemandManually	(A3817)	14.4 -	CACT		
(A3826) KAT CAST On Demand Manually (A3836) AES-CFB128 KAT CAST On Demand Manually (A3847) CAST On Demand Manually	AES-CFB128	KAI	CASI	On Demand	Manually
AES-CFB128KATCASTOn DemandManually(A3836)AES-CFB128KATCASTOn DemandManually	(H3820)		CAST	On Dense d	Maguallu
AES-CFB128 KAT CAST On Demand Manually	AES-CFB128	KAI	CASI	On Demand	Manually
AES-CEBIZØ KAI CASI ON Demand Manually	(A3836)	I/AT	CACT		Manuallu
	AES-CFB128	KA I	CASI	Un Demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-CFB128	КАТ	CAST	On Demand	Manually
(A3854)				-
AES-CTR (A3814)	КАТ	CAST	On Demand	Manually
AES-CTR (A3822)	КАТ	CAST	On Demand	Manually
AES-CTR (A3829)	КАТ	CAST	On Demand	Manually
AES-CTR (A3832)	КАТ	CAST	On Demand	Manually
AES-CTR (A3840)	КАТ	CAST	On Demand	Manually
AES-CTR (A3843)	КАТ	CAST	On Demand	Manually
AES-CTR (A3853)	КАТ	CAST	On Demand	Manually
AES-CTR (A3854)	КАТ	CAST	On Demand	Manually
AES-CTR (A3857)	КАТ	CAST	On Demand	Manually
AES-CTR (A3814)	КАТ	CAST	On Demand	Manually
AES-CTR (A3822)	КАТ	CAST	On Demand	Manually
AES-CTR (A3829)	КАТ	CAST	On Demand	Manually
AES-CTR (A3832)	КАТ	CAST	On Demand	Manually
AES-CTR (A3840)	КАТ	CAST	On Demand	Manually
AES-CTR (A3843)	КАТ	CAST	On Demand	Manually
AES-CTR (A3853)	КАТ	CAST	On Demand	Manually
AES-CTR (A3854)	КАТ	CAST	On Demand	Manually
AES-CTR (A3857)	KAT	CAST	On Demand	Manually
AES-CCM (A3814)	KAT	CAST	On Demand	Manually
AFS-CCM (A3822)	KAT	CAST	On Demand	Manually
AES-CCM (A3829)	KAT	CAST	On Demand	Manually
AES-CCM (A3832)	KAT	CAST	On Demand	Manually
AFS-CCM (A3843)	KAT	CAST	On Demand	Manually
AFS-CCM (A3853)	KAT	CAST	On Demand	Manually
AFS-CCM (A3854)	KAT	CAST	On Demand	Manually
AFS-CCM (A3814)	KAT	CAST	On Demand	Manually
AFS-CCM (A3822)	KAT	CAST	On Demand	Manually
AFS-CCM (A3829)	KAT	CAST	On Demand	Manually
AFS-CCM (A3832)	KAT	CAST	On Demand	Manually
AFS-CCM (A3843)	KAT	CAST	On Demand	Manually
AFS-CCM (A3853)	κάτ	CAST	On Demand	Manually
AFS-CCM (A3854)	κάτ	CAST	On Demand	Manually
ΔFS-GCM (Δ3814)	κδτ	CAST	On Demand	Manually
ΔES-GCM (Δ3820)	κατ	CAST	On Demand	Manually
ΔES-GCM (Δ3821)	κατ	CAST	On Demand	Manually
AFS-GCM (A3822)	ΚΔΤ	CAST	On Demand	Manually
AFS-GCM (A3824)	ΚΔΤ	CAST	On Demand	Manually
AFS-GCM (A3825)	ΚΔΤ	CAST	On Demand	Manually
$\Delta FS-GCM (\Delta 3829)$	κδτ	CAST	On Demand	Manually
AES-GCM (A3830)	κατ	CAST	On Demand	Manually
AES-GCM (A3831)	κατ	CAST	On Demand	Manually
AES (CCM (A3031)	KAT	CAST	On Demand	Manually
AES-CCM (A3833)	KAT	CAST	On Demand	Manually
AES-CCM (A3033)	KAT	CAST	On Demand	Manually
AES-CCM (A3034)	KAT	CAST		Manually
AES-CCM (A3040)		CAST		Manually
AES-CCM (A2041)		CAST		Manually
ALS-UCIM (AS042)		CAST		Manually
AES-UCM (A3843)		CASI		Manually
		CASI		Manually
AES-UCM (AS845)	NAT	CADI		Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-GCM (A3854)	KAT	CAST	On Demand	Manually
AES-GCM (A3855)	КАТ	CAST	On Demand	Manually
AES-GCM (A3856)	КАТ	CAST	On Demand	Manually
AES-GCM (A3814)	КАТ	CAST	On Demand	Manually
AES-GCM (A3820)	KAT	CAST	On Demand	Manually
AES-GCM (A3821)	KAT	CAST	On Demand	Manually
AES-GCM (A3822)	KAT	CAST	On Demand	Manually
AES-GCM (A3824)	KAT	CAST	On Demand	Manually
AES-GCM (A3825)	KAT	CAST	On Demand	Manually
AES-GCM (A3829)	КАТ	CAST	On Demand	Manually
AES-GCM (A3830)	KAT	CAST	On Demand	Manually
AES-GCM (A3831)	KAT	CAST	On Demand	Manually
AES-GCM (A3832)	KAT	CAST	On Demand	Manually
AES-GCM (A3833)	KAT	CAST	On Demand	Manually
AES-GCM (A3834)	КАТ	CAST	On Demand	Manually
AES-GCM (A3840)	КАТ	CAST	On Demand	Manually
AES-GCM (A3841)	КАТ	CAST	On Demand	Manually
AES-GCM (A3842)	КАТ	CAST	On Demand	Manually
AES-GCM (A3843)	КАТ	CAST	On Demand	Manually
AES-GCM (A3844)	КАТ	CAST	On Demand	Manually
AES-GCM (A3845)	КАТ	CAST	On Demand	Manually
AES-GCM (A3854)	КАТ	CAST	On Demand	Manually
AES-GCM (A3855)	КАТ	CAST	On Demand	Manually
AES-GCM (A3856)	КАТ	CAST	On Demand	Manually
AES-OFB (A3818)	КАТ	CAST	On Demand	Manually
AES-OFB (A3827)	КАТ	CAST	On Demand	Manually
AES-OFB (A3837)	КАТ	CAST	On Demand	Manually
AES-OFB (A3848)	КАТ	CAST	On Demand	Manually
AES-OFB (A3854)	КАТ	CAST	On Demand	Manually
AES-OFB (A3818)	КАТ	CAST	On Demand	Manually
AES-OFB (A3827)	КАТ	CAST	On Demand	Manually
AES-OFB (A3837)	КАТ	CAST	On Demand	Manually
AES-OFB (A3848)	КАТ	CAST	On Demand	Manually
AES-OFB (A3854)	КАТ	CAST	On Demand	Manually
AES-XTS Testing	КАТ	CAST	On Demand	Manually
Revision 2.0				
(A3814)	<u> </u>			
AES-XTS Testing	KAT	CAST	On Demand	Manually
Revision 2.0				
(ASOZZ)		CACT	On Domand	Manually
AES-AIS Tesuing	KAT	CASI		Manually
(A 2020)				
ASC29	<i>и</i> лт	CAST	On Demand	Manually
Devision 20	NAT	CASI		Manually
(1 2822)				
AFS-YTS Testing	κδτ	CAST	On Demand	MeuneM
Revision 2.0		CASI		Manually
(A 3840)				
AES-XTS Testing	КАТ	CAST	On Demand	Manually
Revision 2.0				
(A3843)				

ubuntu[©]Canonical Ltd. Ubuntu 22.04 Kernel Crypto API Cryptographic Module FIPS 140-3 Non-Proprietary Security Policy

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-XTS Testing	КАТ	CAST	On Demand	Manually
Revision 2.0				-
(A3853)				
AES-XTS Testing	КАТ	CAST	On Demand	Manually
Revision 2.0				
(A3854)				
AES-XTS Testing	КАТ	CAST	On Demand	Manually
Revision 2.0				
(A3857)				
AES-XTS Testing	КАТ	CAST	On Demand	Manually
Revision 2.0				
(A3814)				
AES-XTS Testing	KAT	CAST	On Demand	Manually
Revision 2.0				
(A3822)				
AES-XTS Testing	КАТ	CAST	On Demand	Manually
Revision 2.0				
(A3829)				
AES-XTS Testing	КАТ	CAST	On Demand	Manually
Revision 2.0				
(A3832)				
AES-XTS Testing	КАТ	CAST	On Demand	Manually
Revision 2.0				
(A3840)				
AES-XTS Testing	КАТ	CAST	On Demand	Manually
Revision 2.0				
(A3843)				
AES-XTS Testing	KAT	CAST	On Demand	Manually
Revision 2.0				
(A3853)				
AES-XTS Testing	КАТ	CAST	On Demand	Manually
Revision 2.0				
(A3854)		- ·		
AES-XTS Testing	KAT	CAST	On Demand	Manually
Revision 2.0				
(A3857)		CACT	On Domond	Maguallu
$\frac{\text{AES-CMAC}(A3814)}{\text{AES-CMAC}(A3822)}$	KAI	CAST	On Demand	Manually
$\frac{AES-CMAC}{AES-CMAC}$	NAT	CAST	On Demand	Manually
$\frac{\text{AES-CMAC}(A3829)}{\text{AES}(A3823)}$		CAST	On Demand	Manually
$\frac{\text{AES-CMAC}(A3832)}{\text{AES}(A3832)}$		CAST	On Demand	Manually
$\frac{\text{AES-CMAC}(A3843)}{\text{AES}(A3853)}$		CAST	On Demand	Manually
$\frac{AES-CMAC}{(A3853)}$	NAT	CAST	On Demand	Manually
AES-CMAC (A3854)	KAI	CAST	On Demand	Manually
SHA-1 (A3812)	KAT	CASI	On Demand	Manually
SHA-1 (A3813)	KAI	CASI	On Demand	Manually
SHA-1 (A3814)	KAI	CASI	Un Demand	Manually
SHA-1 (A3832)	KAI	CASI	On Demand	Manually
SHA-1 (A3850)	KAI	CASI	On Demand	Manually
SHA-1 (A3851)	KAI	CASI	On Demand	Manually
SHA-1 (A3852)	KAI	CASI	On Demand	Manually
SHA-1 (A3853)	KAT	CAST	On Demand	Manually
SHA2-224 (A3812)	KAT	CAST	On Demand	Manually
<u>SHA2-224 (A38</u> 13)	KAT	CAST	On Demand	Manually

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

HMAC-SHA-1 (A3851)KATCASTOn DemandManually (A3852)HMAC-SHA-1 (A3852)KATCASTOn DemandManuallyHMAC-SHA-1 (A3853)KATCASTOn DemandManuallyHMAC-SHA-2224 (A3812)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3813)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3813)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3814)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3832)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3850)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3851)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3852)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3853)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3857)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3853)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3857)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3857)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3853)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3858)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3858)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3858)KATCASTOn Demand </th <th>Algorithm or Test</th> <th>Test Method</th> <th>Test Type</th> <th>Period</th> <th>Periodic Method</th>	Algorithm or Test	Test Method	Test Type	Period	Periodic Method
(A3851)KATCASTOn DemandManuallyHMAC-SHA-1 (A3852)KATCASTOn DemandManuallyHMAC-SHA-1 (A3853)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3813)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3813)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3813)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3814)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3850)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3850)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3851)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3851)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3853)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3853)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3853)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3853)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3853)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3853)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3853)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3858)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3858)KATCASTOn DemandManually </td <td>HMAC-SHA-1</td> <td>КАТ</td> <td>CAST</td> <td>On Demand</td> <td>Manually</td>	HMAC-SHA-1	КАТ	CAST	On Demand	Manually
HMAC-SHA-1 (A3852)KATCASTOn DemandManuallyHMAC-SHA-1 (A3853)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3812)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3813)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3813)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3814)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3814)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3852)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3851)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3851)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3852)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3853)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3853)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3853)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3853)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3853)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3853)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3853)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3858)KATCASTOn DemandManually	(A3851)				-
(A3852)KATCASTOn DemandManually(A3853)HMAC-SHA2-224KATCASTOn DemandManually(A3812)HMAC-SHA2-224KATCASTOn DemandManually(A3813)AAAAAHMAC-SHA2-224KATCASTOn DemandManually(A3813)AAAAAHMAC-SHA2-224KATCASTOn DemandManually(A3814)AAAAAHMAC-SHA2-224KATCASTOn DemandManually(A3832)AAAAAHMAC-SHA2-224KATCASTOn DemandManually(A3850)AAAAAHMAC-SHA2-224KATCASTOn DemandManually(A3852)AAAAAHMAC-SHA2-224KATCASTOn DemandManually(A3853)AAAAAHMAC-SHA2-224KATCASTOn DemandManually(A3853)AAAAAHMAC-SHA2-224KATCASTOn DemandManually(A3853)AAAAAHMAC-SHA2-224KATCASTOn DemandManually(A3853)AAAAAHMAC-SHA2-224KATCASTOn DemandManually(A3853)AAAAA	HMAC-SHA-1	КАТ	CAST	On Demand	Manually
HMAC-SHA-1 (A3853)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3812)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3813)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3813)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3814)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3812)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3832)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3850)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3851)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3851)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3853)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3853)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3853)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3853)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3857)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3858)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3858)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3858)KATCASTOn DemandManually	(A3852)				
(A3853)CASTOn DemandManuallyHMAC-SHA2-224 (A3812)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3813)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3814)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3812)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3822)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3850)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3851)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3851)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3853)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3853)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3853)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3853)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3853)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3853)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3858)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3858)KATCASTOn DemandManually	HMAC-SHA-1	KAT	CAST	On Demand	Manually
HMAC-SHA2-224 (A3812)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3813)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3814)KATCASTOn DemandManuallyHMAC-SHA2-224 (A382)KATCASTOn DemandManuallyHMAC-SHA2-224 (A382)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3850)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3851)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3851)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3852)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3853)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3853)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3853)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3853)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3853)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3857)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3858)KATCASTOn DemandManually	(A3853)				
(A3812)KATCASTOn DemandManuallyHMAC-SHA2-224KATCASTOn DemandManually(A3813)HMAC-SHA2-224KATCASTOn DemandManually(A3814)HMAC-SHA2-224KATCASTOn DemandManually(A382)HMAC-SHA2-224KATCASTOn DemandManually(A3850)HMAC-SHA2-224KATCASTOn DemandManually(A3851)HMAC-SHA2-224KATCASTOn DemandManually(A3852)HMAC-SHA2-224KATCASTOn DemandManually(A3853)HMAC-SHA2-224KATCASTOn DemandManually(A3853)ATCASTOn DemandManually(A3853)ATCASTOn DemandManually(A3853)ATCASTOn DemandManually(A3853)ATCASTOn DemandManually(A3853)ATCASTOn DemandManually(A3853)ATCASTOn DemandManually(A3853)ATCASTOn DemandManually(A3857)ATCASTOn DemandManuallyHMAC-SHA2-224KATCASTOn DemandManually(A3858)ATCASTOn DemandManually	HMAC-SHA2-224	КАТ	CAST	On Demand	Manually
HMAC-SHA2-224 (A3813)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3814)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3832)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3850)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3850)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3851)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3851)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3852)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3853)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3853)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3857)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3858)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3858)KATCASTOn DemandManually	(A3812)				-
(A3813)CASTOn DemandManuallyHMAC-SHA2-224KATCASTOn DemandManuallyHMAC-SHA2-224KATCASTOn DemandManually(A3832)HMAC-SHA2-224KATCASTOn DemandManually(A3850)HMAC-SHA2-224KATCASTOn DemandManually(A3851)HMAC-SHA2-224KATCASTOn DemandManually(A3852)HMAC-SHA2-224KATCASTOn DemandManually(A3852)HMAC-SHA2-224KATCASTOn DemandManually(A3853)HMAC-SHA2-224KATCASTOn DemandManually(A3853)HMAC-SHA2-224KATCASTOn DemandManually(A3857)KATCASTOn DemandManually(A3858)KATCASTOn DemandManually	HMAC-SHA2-224	КАТ	CAST	On Demand	Manually
HMAC-SHA2-224 (A3814)KATCASTOn DemandManually (A3814)HMAC-SHA2-224 (A3832)KATCASTOn DemandManually (A3830)HMAC-SHA2-224 (A3850)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3851)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3851)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3852)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3853)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3853)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3853)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3857)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3858)KATCASTOn DemandManually	(A3813)				
(A3814)ATCASTOn DemandManuallyHMAC-SHA2-224KATCASTOn DemandManually(A3850)ATCASTOn DemandManuallyHMAC-SHA2-224KATCASTOn DemandManually(A3851)KATCASTOn DemandManuallyHMAC-SHA2-224KATCASTOn DemandManually(A3851)KATCASTOn DemandManuallyHMAC-SHA2-224KATCASTOn DemandManually(A3852)ATCASTOn DemandManuallyHMAC-SHA2-224KATCASTOn DemandManually(A3853)ATCASTOn DemandManuallyHMAC-SHA2-224KATCASTOn DemandManually(A3857)ATCASTOn DemandManuallyHMAC-SHA2-224KATCASTOn DemandManually(A3858)ATCASTOn DemandManually	HMAC-SHA2-224	КАТ	CAST	On Demand	Manually
HMAC-SHA2-224 (A3832)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3850)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3851)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3851)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3852)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3853)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3853)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3857)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3858)KATCASTOn DemandManually	(A3814)				
(A3832)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3850)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3851)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3852)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3853)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3853)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3857)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3857)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3858)KATCASTOn DemandManually	HMAC-SHA2-224	КАТ	CAST	On Demand	Manually
HMAC-SHA2-224 (A3850)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3851)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3852)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3853)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3853)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3857)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3857)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3858)KATCASTOn DemandManually	(A3832)				
(A3850)KATCASTOn DemandManually(A3851)HMAC-SHA2-224KATCASTOn DemandManually(A3852)HMAC-SHA2-224KATCASTOn DemandManually(A3853)HMAC-SHA2-224KATCASTOn DemandManually(A3857)HMAC-SHA2-224KATCASTOn DemandManually(A3857)HMAC-SHA2-224KATCASTOn DemandManually(A3858)Image: Cast of the second sec	HMAC-SHA2-224	КАТ	CAST	On Demand	Manually
HMAC-SHA2-224 (A3851)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3852)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3853)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3853)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3857)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3857)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3858)KATCASTOn DemandManually	(A3850)				
(A3851)CASTOn DemandManuallyHMAC-SHA2-224 (A3852)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3853)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3857)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3857)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3858)KATCASTOn DemandManually	HMAC-SHA2-224	КАТ	CAST	On Demand	Manually
HMAC-SHA2-224 (A3852)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3853)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3857)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3857)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3858)KATCASTOn DemandManually	(A3851)				
(A3852)CASTOn DemandManuallyHMAC-SHA2-224 (A3853)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3857)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3858)KATCASTOn DemandManually	HMAC-SHA2-224	КАТ	CAST	On Demand	Manually
HMAC-SHA2-224 (A3853)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3857)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3858)KATCASTOn DemandManually	(A3852)				
(A3853)KATCASTOn DemandManually(A3857)HMAC-SHA2-224KATCASTOn DemandManually(A3858)Image: Cast of the second seco	HMAC-SHA2-224	КАТ	CAST	On Demand	Manually
HMAC-SHA2-224 (A3857)KATCASTOn DemandManuallyHMAC-SHA2-224 (A3858)KATCASTOn DemandManually	(A3853)				
(A3857) CAST On Demand Manually (A3858) (A3858) (A3858) (A3858) (A3858) (A3858)	HMAC-SHA2-224	КАТ	CAST	On Demand	Manually
HMAC-SHA2-224 KAT CAST On Demand Manually (A3858)	(A3857)				
(A3858)	HMAC-SHA2-224	КАТ	CAST	On Demand	Manually
	(A3858)				
HMAC-SHA2-256 KAT CAST On Demand Manually	HMAC-SHA2-256	КАТ	CAST	On Demand	Manually
(A3812)	(A3812)				
HMAC-SHA2-256 KAT CAST On Demand Manually	HMAC-SHA2-256	КАТ	CAST	On Demand	Manually
(A3813)	(A3813)				
HMAC-SHA2-256 KAT CAST On Demand Manually	HMAC-SHA2-256	KAT	CAST	On Demand	Manually
(A3814)	(A3814)				
HMAC-SHA2-256 KAT CAST On Demand Manually	HMAC-SHA2-256	КАТ	CAST	On Demand	Manually
(A3832)	(A3832)				
HMAC-SHA2-256 KAT CAST On Demand Manually	HMAC-SHA2-256	КАТ	CAST	On Demand	Manually
(A3850)	(A3850)				
HMAC-SHA2-256 KAT CAST On Demand Manually	HMAC-SHA2-256	КАТ	CAST	On Demand	Manually
	(A3851)				
HMAC-SHA2-256 KAT CAST On Demand Manually	HMAC-SHA2-256	KAI	CASI	On Demand	Manually
	(A3852)	1/A 7	0.1.0 T		
HMAC-SHA2-256 KAT CAST On Demand Manually	HMAC-SHA2-256	KAI	CASI	On Demand	Manually
	(A3853)	1/ A T	CACT		
HMAC-SHA2-256 KAT CAST On Demand Manually	HMAC-SHA2-256	KAT	CAST	On Demand	Manually
	(A3857)	1/ 4 T	CACT		A
HMAC-SHA2-256 KAT CAST ON Demand Manually	HMAC-SHAZ-256	KAT	CASI	On Demand	Manually
	(A3858)	1/ A T	CACT		
		KA I	CASI	Un Demañd	Manually
		илт.	CAST	On Domand	Manually
	1111AC-3HAZ-384	NA I	CASI		manually
		νλτ	CAST	On Domand	Manually
	1 11VIAC-304 (A 2014)		CASI		manually
		νλτ	CAST	On Domand	Manually
	(A 3832)				

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
HMAC-SHA2-384	КАТ	CAST	On Demand	Manually
(A3850)				_
HMAC-SHA2-384	КАТ	CAST	On Demand	Manually
(A3851)				
HMAC-SHA2-384	KAT	CAST	On Demand	Manually
(A3852)				
HMAC-SHA2-384	КАТ	CAST	On Demand	Manually
(A3858)				
HMAC-SHA2-512	КАТ	CAST	On Demand	Manually
(A3812)				
HMAC-SHA2-512	КАТ	CAST	On Demand	Manually
(A3813)				
HMAC-SHA2-512	КАТ	CAST	On Demand	Manually
(A3814)				
HMAC-SHA2-512	КАТ	CAST	On Demand	Manually
(A3832)				
HMAC-SHA2-512	КАТ	CAST	On Demand	Manually
(A3850)				
HMAC-SHA2-512	КАТ	CAST	On Demand	Manually
(A3851)				
HMAC-SHA2-512	КАТ	CAST	On Demand	Manually
(A3852)				
HMAC-SHA2-512	КАТ	CAST	On Demand	Manually
(A3858)				
HMAC-SHA3-224	KAI	CAST	On Demand	Manually
(A3816)	1/A T	0.4.0 		
HMAC-SHA3-224	KAT	CAST	On Demand	Manually
(A3839)		CACT	On Daman d	
	KAT	CAST	On Demand	Manually
		CAST	On Domand	Manually
	NAT	CASI	On Demand	Manually
		CAST	On Domand	Manually
∏MAC-3ΠA3-364	NAT	CASI	On Demand	Manually
	KAT	CAST	On Domand	Manually
(110/AC-51/A5-504	NA I	CASI		Manually
HMAC-SHA3-512	κατ	CAST	On Demand	Manually
(A 3816)		CASI		Mandatty
HMAC-SHA3-512	КАТ	CAST	On Demand	Manually
(A 3839)				hencetty
Counter DRBG	КАТ	CAST	On Demand	Manually
(A3812)		C/ (S1		handetty
Counter DRBG	КАТ	CAST	On Demand	Manually
(A3813)				
Counter DRBG	КАТ	CAST	On Demand	Manually
(A3814)				, , , , , , , , , , , , , , , , , , ,
Counter DRBG	КАТ	CAST	On Demand	Manually
(A3820)				
Counter DRBG	КАТ	CAST	On Demand	Manually
(A3821)				_
Counter DRBG	КАТ	CAST	On Demand	Manually
(A3822)				
Counter DRBG	КАТ	CAST	On Demand	Manually
(A3824)				

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
Counter DRBG (A3825)	КАТ	CAST	On Demand	Manually
Counter DRBG (A3829)	КАТ	CAST	On Demand	Manually
Counter DRBG	КАТ	CAST	On Demand	Manually
Counter DRBG	КАТ	CAST	On Demand	Manually
Counter DRBG	КАТ	CAST	On Demand	Manually
Counter DRBG	КАТ	CAST	On Demand	Manually
Counter DRBG	КАТ	CAST	On Demand	Manually
Counter DRBG	КАТ	CAST	On Demand	Manually
Counter DRBG	КАТ	CAST	On Demand	Manually
Counter DRBG	КАТ	CAST	On Demand	Manually
Counter DRBG	КАТ	CAST	On Demand	Manually
Counter DRBG (A3844)	КАТ	CAST	On Demand	Manually
Counter DRBG	КАТ	CAST	On Demand	Manually
Counter DRBG	КАТ	CAST	On Demand	Manually
Counter DRBG (A3855)	КАТ	CAST	On Demand	Manually
Counter DRBG	КАТ	CAST	On Demand	Manually
Hash DRBG (A3812)	КАТ	CAST	On Demand	Manually
Hash DRBG (A3813)	KAT	CAST	On Demand	Manually
Hash DRBG (A3814)	KAT	CAST	On Demand	Manually
Hash DRBG (A3820)	KAT	CAST	On Demand	Manually
Hash DRBG (A3821)	ΚΔΤ	CAST	On Demand	Manually
Hash DRBG (A3822)	КАТ	CAST	On Demand	Manually
Hash DRBG (A3824)	KAT	CAST	On Demand	Manually
Hash DRBG (A3825)	KAT	CAST	On Demand	Manually
Hash DRBG (A3830)	КАТ	CAST	On Demand	Manually
Hash DRBG (A3831)	КАТ	CAST	On Demand	Manually
Hash DRBG (A3832)	КАТ	CAST	On Demand	Manually
Hash DRBG (A3833)	ΚΔΤ	CAST	On Demand	Manually
Hash DRBG (A3834)	κατ	CAST	On Demand	Manually
Hash DRBG (A38/0)	κδτ	CAST	On Demand	Manually
Hash DRBC (A38/1)	ΚΔΤ	CAST	On Demand	Manually
Hach DDBC (A3041)	KAT	CAST	On Demand	Manually
Hach DDBC (A2042)	KAT	CAST	On Demand	Manually
Hach DDBC (A2043)	KAT	CAST	On Demand	Manually
Hach DDBC (A2044)	KAT	CAST		Manually
		CAST	On Demand	Manually
Hash DRBG (A3851)	ΚΔΤ	CAST	On Demand	Manually
				manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
Hash DRBG (A3852)	КАТ	CAST	On Demand	Manually
Hash DRBG (A3855)	КАТ	CAST	On Demand	Manually
Hash DRBG (A3856)	КАТ	CAST	On Demand	Manually
HMAC DRBG	КАТ	CAST	On Demand	Manually
(A3812)				
HMAC DRBG	КАТ	CAST	On Demand	Manually
(A3813)				
HMAC DRBG	КАТ	CAST	On Demand	Manually
(A3814)				-
HMAC DRBG	КАТ	CAST	On Demand	Manually
(A3820)				
HMAC DRBG	КАТ	CAST	On Demand	Manually
(A3821)				-
HMAC DRBG	КАТ	CAST	On Demand	Manually
(A3822)				-
HMAC DRBG	КАТ	CAST	On Demand	Manually
(A3824)				-
HMAC DRBG	КАТ	CAST	On Demand	Manually
(A3825)				_
HMAC DRBG	КАТ	CAST	On Demand	Manually
(A3830)				_
HMAC DRBG	KAT	CAST	On Demand	Manually
(A3831)				
HMAC DRBG	КАТ	CAST	On Demand	Manually
(A3832)				
HMAC DRBG	КАТ	CAST	On Demand	Manually
(A3833)				
HMAC DRBG	KAT	CAST	On Demand	Manually
(A3834)				
HMAC DRBG	КАТ	CAST	On Demand	Manually
(A3840)				
HMAC DRBG	КАТ	CAST	On Demand	Manually
(A3841)				
HMAC DRBG	KAT	CAST	On Demand	Manually
(A3842)				
HMAC DRBG	КАТ	CAST	On Demand	Manually
(A3843)				
HMAC DRBG	KAT	CAST	On Demand	Manually
(A3844)				
HMAC DRBG	КАТ	CAST	On Demand	Manually
(A3845)				
HMAC DRBG	KAT	CAST	On Demand	Manually
(A3850)				
HMAC DRBG	КАТ	CAST	On Demand	Manually
(A3851)				
HMAC DRBG	KAT	CAST	On Demand	Manually
(A3852)	14.4 -	6 4 6 7		
	KAT	CASI	On Demand	Manually
(A3855)				
	KAI	CASI	On Demand	Manually
(A3856)		CACT	On Deers and	Manually
KAS-ELL-SSL	KAT	CASI	Un Demand	Manually
2000-20AF3				
(A3813)				

ubuntu[©]Canonical Ltd. Ubuntu 22.04 Kernel Crypto API Cryptographic Module FIPS 140-3 Non-Proprietary Security Policy

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
KAS-FFC-SSC Sp800-56Ar3 (A3812)	КАТ	CAST	On Demand	Manually
RSA SigVer (FIPS186-4) (A3814)	КАТ	CAST	On Demand	Manually
RSA SigVer (FIPS186-4) (A3832)	КАТ	CAST	On Demand	Manually
RSA SigVer (FIPS186-4) (A3850)	КАТ	CAST	On Demand	Manually
RSA SigVer (FIPS186-4) (A3851)	КАТ	CAST	On Demand	Manually
RSA SigVer (FIPS186-4) (A3852)	КАТ	CAST	On Demand	Manually
Safe Primes Key Generation (A3812)	РСТ	РСТ	On Demand	Manually
ECDSA KeyGen (FIPS186-4) (A3813)	РСТ	РСТ	On Demand	Manually
Entropy Source	RCT	CAST	On Demand	Manually
Entropy Source	APT	CAST	On Demand	Manually
Entropy Source	RCT	CAST	On Demand	Manually
Entropy Source	APT	CAST	On Demand	Manually

Table 23: Conditional Periodic Information

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
Error	The Linux kernel immediately stops	Any self-test	Restart of the	Kernel
State	executing	failure	module	Panic
Table 24 Free Chabas				

Table 24: Error States

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

10.5 Operator Initiation of Self-Tests

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

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

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

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

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

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

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

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

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

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

\$ cat /proc/sys/crypto/fips_name

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

Ubuntu 22.04 Kernel Crypto API Cryptographic Module

Then, the Crypto Officer must execute:

\$ cat /proc/sys/crypto/fips_version

This command must output the following:

5.15.0-73-fips

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

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

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

\$ snap list fips-kernel

11.2 Administrator Guidance

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

11.3 Non-Administrator Guidance

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

11.4 End of Life

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

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

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

ubuntu[©]Canonical Ltd. Ubuntu 22.04 Kernel Crypto API Cryptographic Module FIPS 140-3 Non-Proprietary Security Policy

12 Mitigation of Other Attacks

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

Appendix A. Glossary and Abbreviations

AES API CAST CAVP	Advanced Encryption Standard Application Programming Interface Cryptographic Algorithm Self-Test Cryptographic Algorithm Validation Program
CBC CCM CFB	Cipher Block Chaining Counter with Cipher Block Chaining-Message Authentication Code 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	Кеу Шгар
MAC	Message Authentication Code
NIST	National Institute of Science and Technology
OFB	Output Feedback
PAA	Processor Algorithm Acceleration
PAI	Processor Algorithm Implementation
PCT	Pair-wise Consistency Test
PBKDF2	Password-based Key Derivation Function v2
PKCS	Public-Key Cryptography Standards
RSA	Rivest, Shamir, Addleman
SHA	Secure Hash Algorithm
SSC	Shared Secret Computation
SSP	Sensitive Security Parameter
XTS	XEX-based Tweaked-codebook mode with cipher text Stealing

Appendix B. References

FIPS 140-3	FIPS PUB 140-3 - Security Requirements For Cryptographic Modules March 2019
	https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-3.pdf
FIPS 140-3 IG	Implementation Guidance for FIPS PUB 140-3 and the Cryptographic Module Validation Program https://csrc.nist.gov/Projects/cryptographic-module-validation- program/fips-140-3-ig-announcements
FIPS 180-4	Secure Hash Standard (SHS) March 2012 https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf
FIPS 186-4	Digital Signature Standard (DSS) July 2013 https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf
FIPS 186-5	Digital Signature Standard (DSS) February 2023 https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-5.pdf
FIPS 197	Advanced Encryption Standard November 2001 https://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
FIPS 198-1	The Keyed Hash Message Authentication Code (HMAC) July 2008 https://csrc.nist.gov/publications/fips/fips198-1/FIPS-198-1_final.pdf
FIPS 202	SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions August 2015 https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf
PKCS#1	Public Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1 February 2003 https://www.ietf.org/rfc/rfc3447.txt
RFC 3526	More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE) May 2003 https://www.ietf.org/rfc/rfc3526.txt
RFC 4106	The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP) June 2005 https://datatracker.ietf.org/doc/html/rfc4106
RFC 7296	Internet Key Exchange Protocol Version 2 (IKEv2) October 2014 https://datatracker.ietf.org/doc/html/rfc7296

SP 800-38A	Recommendation for Block Cipher Modes of Operation Methods and Techniques December 2001 https://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf
SP 800-38A Addendum	Recommendation for Block Cipher Modes of Operation: Three Variants of Ciphertext Stealing for CBC Mode October 2010
	https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800- 38a-add.pdf
SP 800-38B	Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication May 2005 https://csrc.nist.gov/publications/nistpubs/800-38B/SP_800-38B.pdf
SP 800-38C	Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality May 2004 https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800- 38c.pdf
SP 800-38D	Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC November 2007 https://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf
SP 800-38E	Recommendation for Block Cipher Modes of Operation: The XTS AES Mode for Confidentiality on Storage Devices January 2010 https://csrc.nist.gov/publications/nistpubs/800-38E/nist-sp-800-38E.pdf
SP 800-38F	Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping December 2012 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800- 38F.pdf
SP 800-56Ar3	Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography April 2018 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800- 56Ar3.pdf
SP 800-90Ar1	Recommendation for Random Number Generation Using Deterministic Random Bit Generators June 2015 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800- 90Ar1.pdf
SP 800-90B	Recommendation for the Entropy Sources Used for Random Bit Generation January 2018 <u>https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-</u> 90B.pdf

SP 800-133r2Recommendation for Cryptographic Key Generation
June 2020
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-
133r2.pdfSP 800-140Br1CMVP Security Policy Requirements

March 2020 <u>https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-</u> <u>140Br1.pdf</u>