



Canonical Ltd.

Canonical Ltd. Ubuntu 22.04 OpenSSL Cryptographic Module

FIPS 140-3 Non-Proprietary Security Policy

Document Version: 1.1

Last Updated: 2024-08-28

Prepared by:

atsec information security corporation
4516 Seton Center Parkway, Suite 250

Austin, TX 78759

www.atsec.com

Prepared for:

Canonical Ltd.

110 Southwark Street, Blue Fin Building,
5th Floor

London, SE1 0SU

www.canonical.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	32
2.7 Algorithm Specific Information	44
2.7.1 AES GCM IV.....	44
2.7.2 AES XTS	45
2.7.3 Key Derivation using SP 800-132 PBKDF2	45
2.7.4 Compliance to SP 800-56Arev3 Assurances	46
2.7.5 Legacy Algorithms.....	46
2.8 RBG and Entropy.....	46
2.9 Key Generation.....	47
2.10 Key Establishment.....	48
2.11 Industry Protocols	48
2.12 Additional Information	49
3 Cryptographic Module Interfaces.....	50
3.1 Ports and Interfaces	50
3.2 Trusted Channel Specification	50
3.3 Control Interface Not Inhibited	50
3.4 Additional Information	50
4 Roles, Services, and Authentication	51
4.1 Authentication Methods	51
4.2 Roles.....	51
4.3 Approved Services	51
4.4 Non-Approved Services	59
4.5 External Software/Firmware Loaded.....	59
4.6 Bypass Actions and Status	59
4.7 Cryptographic Output Actions and Status	60
4.8 Additional Information	60

5 Software/Firmware Security	61
5.1 Integrity Techniques	61
5.2 Initiate on Demand	61
5.3 Open-Source Parameters	61
5.4 Additional Information	61
6 Operational Environment	62
6.1 Operational Environment Type and Requirements	62
6.2 Configuration Settings and Restrictions	62
6.3 Additional Information	62
7 Physical Security	63
7.1 Mechanisms and Actions Required	63
7.2 User Placed Tamper Seals	63
7.3 Filler Panels	63
7.4 Fault Induction Mitigation	63
7.5 EFP/EFT Information	63
7.6 Hardness Testing Temperature Ranges	63
7.7 Additional Information	64
8 Non-Invasive Security	65
8.1 Mitigation Techniques	65
8.2 Effectiveness	65
8.3 Additional Information	65
9 Sensitive Security Parameters Management	66
9.1 Storage Areas	66
9.2 SSP Input-Output Methods	66
9.3 SSP Zeroization Methods	66
9.4 SSPs	67
9.5 Transitions	73
9.6 Additional Information	73
10 Self-Tests	74
10.1 Pre-Operational Self-Tests	74
10.2 Conditional Self-Tests	75
10.3 Periodic Self-Test Information	89
10.4 Error States	96
10.5 Operator Initiation of Self-Tests	97
10.6 Additional Information	97
11 Life-Cycle Assurance	98
11.1 Installation, Initialization, and Startup Procedures	98

11.2 Administrator Guidance	99
11.3 Non-Administrator Guidance	99
11.4 Design and Rules	99
11.5 Maintenance Requirements	99
11.6 End of Life.....	99
11.7 Additional Information	99
12 Mitigation of Other Attacks	100
12.1 Attack List	100
12.2 Mitigation Effectiveness	100
12.3 Guidance and Constraints	100
12.4 Additional Information	100
Appendix A. Glossary and Abbreviations.....	101
Appendix B. References	103

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.....	31
Table 6: Vendor-Affirmed Algorithms.....	31
Table 7: Non-Approved, Not Allowed Algorithms	32
Table 8: Security Function Implementations	44
Table 9: Entropy Certificates	46
Table 10: Entropy Sources.....	46
Table 11: Ports and Interfaces.....	50
Table 12: Roles	51
Table 13: Approved Services	58
Table 14: Non-Approved Services	59
Table 15: EFP/EFT Information.....	63
Table 16: Hardness Testing Temperatures	63
Table 17: Storage Areas.....	66
Table 18: SSP Input-Output Methods.....	66
Table 19: SSP Zeroization Methods	67
Table 20: SSP Table 1.....	69
Table 21: SSP Table 2.....	72
Table 22: Pre-Operational Self-Tests	74
Table 23: Conditional Self-Tests.....	89
Table 24: Pre-Operational Periodic Information	90
Table 25: Conditional Periodic Information	96
Table 26: Error States.....	96

List of Figures

Figure 1: Block Diagram.....	8
------------------------------	---

1 General

1.1 Overview

This document is the non-proprietary FIPS 140-3 Security Policy for version 3.0.5-0ubuntu0.1+Fips2.1 of the Canonical Ltd. Ubuntu 22.04 OpenSSL 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	1
	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 OpenSSL Cryptographic Module (hereafter referred to as “the module”) is defined as a software module in a multi-chip standalone embodiment. It provides a C language application program interface (API) for use by other applications that require cryptographic functionality. The module consists of one software component, the “FIPS provider” i.e., fips.so, which implements the FIPS requirements and the cryptographic functionality provided to the operator.

Module Type: Software

Module Embodiment: MultiChipStand

Module Characteristics:

Cryptographic Boundary:

Components in white are only included in the diagram for informational purposes. They are not included in the cryptographic boundary (and therefore not part of the module’s validation). For example, the kernel is responsible for managing system calls issued by the module itself, as well as other applications using the module for cryptographic services.

Tested Operational Environment’s Physical Perimeter (TOEPP):

Figure 1 shows a block diagram that represents the design of the module when the module is operational and providing services to other user space applications. In this diagram, the physical perimeter of the operational environment (a general-purpose computer on which the module is installed) is indicated by a purple dashed line. The cryptographic boundary is represented by the components painted in orange blocks, which consists only of the shared library implementing the FIPS provider (fips.so).

Green lines indicate the flow of data between the cryptographic module and its operator application, through the logical interfaces defined in Section 3.

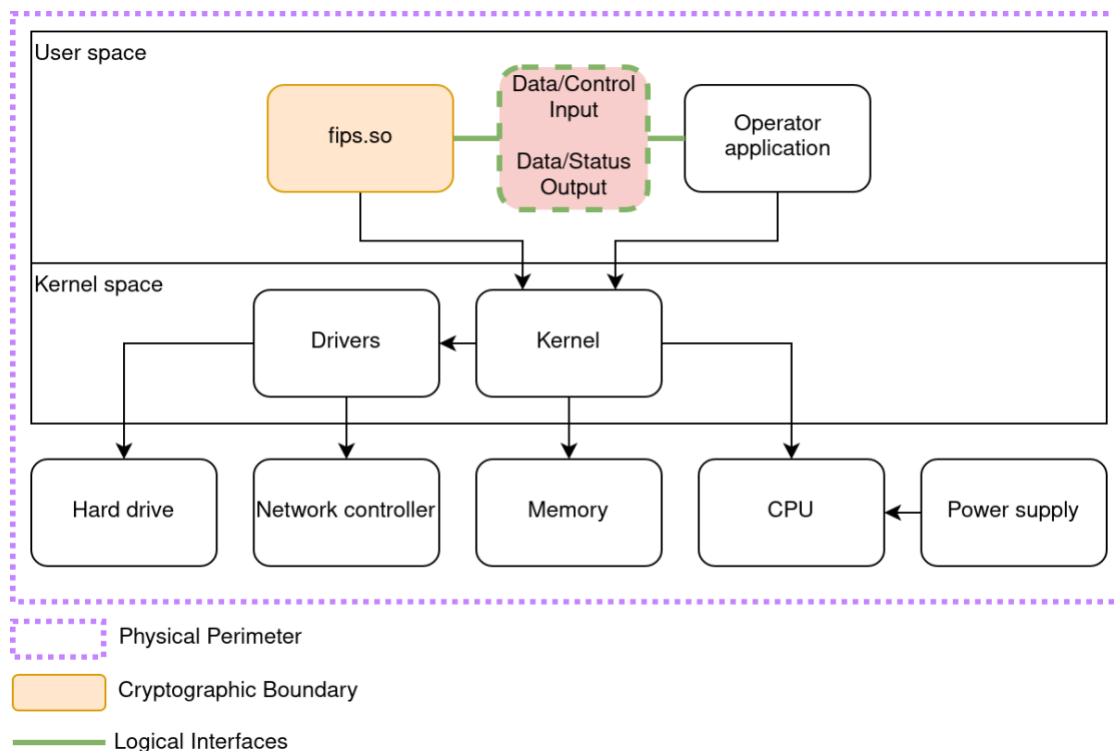


Figure 1: Block Diagram

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
fips.so on Ubuntu 22.04 with Intel Xeon Gold 6226	3.0.5-0ubuntu0.1+Fips2.1	N/A	HMAC-SHA2-256
fips.so on Ubuntu 22.04 with AWS Graviton2	3.0.5-0ubuntu0.1+Fips2.1	N/A	HMAC-SHA2-256
fips.so on Ubuntu 22.04 with IBM z15	3.0.5-0ubuntu0.1+Fips2.1	N/A	HMAC-SHA2-256

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:

© 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	Supermicro SYS-1019P-WTR	Intel Xeon Gold 6226	Yes	N/A	3.0.5-0ubuntu0.1+Fips2.1
Ubuntu 22.04	Amazon Web Services (AWS) c6g.metal	AWS Graviton2	Yes	N/A	3.0.5-0ubuntu0.1+Fips2.1
Ubuntu 22.04	IBM z15	IBM z15	Yes	N/A	3.0.5-0ubuntu0.1+Fips2.1
Ubuntu 22.04	Supermicro SYS-1019P-WTR	Intel Xeon Gold 6226	No	N/A	3.0.5-0ubuntu0.1+Fips2.1
Ubuntu 22.04	Amazon Web Services (AWS) c6g.metal	AWS Graviton2	No	N/A	3.0.5-0ubuntu0.1+Fips2.1
Ubuntu 22.04	IBM z15	IBM z15	No	N/A	3.0.5-0ubuntu0.1+Fips2.1

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

There are no components excluded from the module.

2.4 Modes of Operation

Modes List and Description:

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

Table 4: Modes List and Description

The module supports two modes of operation: (1) the approved mode of operation, in which the approved or vendor affirmed services are available as specified in the Approved Services table and (2) the non-approved mode of operation, in which the non-approved services are available as specified in the Non-Approved Services table.

Mode Change Instructions and Status:

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

Degraded Mode Description:

© 2024 Canonical Ltd. / atsec information security.

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

The module does not implement a degraded mode of operation.

2.5 Algorithms

Approved Algorithms:

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	A3958	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CBC-CS1	A3958	Direction - decrypt, encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CBC-CS2	A3958	Direction - decrypt, encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CBC-CS3	A3958	Direction - decrypt, encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CCM	A3958	Key Length - 128, 192, 256	SP 800-38C
AES-CFB1	A3958	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CFB128	A3958	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CFB8	A3958	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CMAC	A3958	Direction - Generation, Verification Key Length - 128, 192, 256	SP 800-38B
AES-CTR	A3958	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-ECB	A3958	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-KW	A3958	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38F
AES-KWP	A3958	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38F
AES-OFB	A3958	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-XTS Testing Revision 2.0	A3958	Direction - Decrypt, Encrypt Key Length - 128, 256	SP 800-38E
AES-CBC	A3959	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CBC-CS1	A3959	Direction - decrypt, encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CBC-CS2	A3959	Direction - decrypt, encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CBC-CS3	A3959	Direction - decrypt, encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CCM	A3959	Key Length - 128, 192, 256	SP 800-38C
AES-CFB1	A3959	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A

Algorithm	CAVP Cert	Properties	Reference
AES-CFB128	A3959	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CFB8	A3959	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CMAC	A3959	Direction - Generation, Verification Key Length - 128, 192, 256	SP 800-38B
AES-CTR	A3959	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-ECB	A3959	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-KW	A3959	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38F
AES-KWP	A3959	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38F
AES-OFB	A3959	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-XTS Testing Revision 2.0	A3959	Direction - Decrypt, Encrypt Key Length - 128, 256	SP 800-38E
AES-CBC	A3960	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CBC-CS1	A3960	Direction - decrypt, encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CBC-CS2	A3960	Direction - decrypt, encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CBC-CS3	A3960	Direction - decrypt, encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CCM	A3960	Key Length - 128, 192, 256	SP 800-38C
AES-CFB1	A3960	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CFB128	A3960	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CFB8	A3960	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CMAC	A3960	Direction - Generation, Verification Key Length - 128, 192, 256	SP 800-38B
AES-CTR	A3960	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-ECB	A3960	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-KW	A3960	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38F
AES-KWP	A3960	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38F
AES-OFB	A3960	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A

Algorithm	CAVP Cert	Properties	Reference
AES-XTS Testing Revision 2.0	A3960	Direction - Decrypt, Encrypt Key Length - 128, 256	SP 800-38E
AES-GCM	A3961	Direction - Decrypt, Encrypt IV Generation - External, Internal IV Generation Mode - 8.2.1 Key Length - 128, 192, 256	SP 800-38D
AES-GMAC	A3961	Direction - Decrypt, Encrypt IV Generation - External IV Generation Mode - 8.2.1 Key Length - 128, 192, 256	SP 800-38D
ECDSA KeyGen (FIPS186-4)	A3962	Curve - P-224, P-256, P-384, P-521 Secret Generation Mode - Testing Candidates	FIPS 186-4
ECDSA KeyVer (FIPS186-4)	A3962	Curve - P-224, P-256, P-384, P-521	FIPS 186-4
ECDSA SigGen (FIPS186-4)	A3962	Component - No Curve - P-224, P-256, P-384, P-521 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256	FIPS 186-4
ECDSA SigVer (FIPS186-4)	A3962	Component - No Curve - P-192, P-224, P-256, P-384, P-521 Hash Algorithm - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256	FIPS 186-4
HMAC-SHA-1	A3962	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-224	A3962	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-256	A3962	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-384	A3962	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-512	A3962	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-512/224	A3962	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-512/256	A3962	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
KAS-ECC-SSC Sp800-56Ar3	A3962	Domain Parameter Generation Methods - P-224, P-256, P-384, P-521 Scheme - ephemeralUnified - KAS Role - initiator, responder	SP 800-56A Rev. 3
KDF ANS 9.42 (CVL)	A3962	KDF Type - DER Hash Algorithm - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256 Key Data Length - Key Data Length: 112-4096 Increment 8	SP 800-135 Rev. 1
KDF ANS 9.63 (CVL)	A3962	Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256 Key Data Length - Key Data Length: 128-4096 Increment 8	SP 800-135 Rev. 1

Algorithm	CAVP Cert	Properties	Reference
PBKDF	A3962	Iteration Count - Iteration Count: 1000-10000 Increment 1 Password Length - Password Length: 8-128 Increment 1	SP 800-132
RSA KeyGen (FIPS186-4)	A3962	Key Generation Mode - B.3.6 Modulo - 2048, 3072, 4096 Primality Tests - Table C.2 Private Key Format - Standard	FIPS 186-4
RSA SigGen (FIPS186-4)	A3962	Signature Type - PKCS 1.5, PKCSPSS Modulo - 2048, 3072, 4096	FIPS 186-4
RSA SigVer (FIPS186-4)	A3962	Signature Type - PKCS 1.5, PKCSPSS Modulo - 1024, 2048, 3072, 4096	FIPS 186-4
SHA-1	A3962	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 180-4
SHA2-224	A3962	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 180-4
SHA2-256	A3962	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 180-4
SHA2-384	A3962	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 180-4
SHA2-512	A3962	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 180-4
SHA2-512/224	A3962	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 180-4
SHA2-512/256	A3962	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 180-4
TLS v1.2 KDF RFC7627 (CVL)	A3962	Hash Algorithm - SHA2-256, SHA2-384, SHA2-512	SP 800-135 Rev. 1
HMAC-SHA2-256	A3963	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
SHA2-256	A3963	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 180-4
ECDSA SigGen (FIPS186-4)	A3964	Component - No Curve - P-224, P-256, P-384, P-521 Hash Algorithm - SHA3-224, SHA3-256, SHA3-384, SHA3-512	FIPS 186-4
ECDSA SigVer (FIPS186-4)	A3964	Component - No Curve - P-192, P-224, P-256, P-384, P-521 Hash Algorithm - SHA3-224, SHA3-256, SHA3-384, SHA3-512	FIPS 186-4
HMAC-SHA3-224	A3964	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA3-256	A3964	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA3-384	A3964	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA3-512	A3964	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1

Algorithm	CAVP Cert	Properties	Reference
KDF ANS 9.42 (CVL)	A3964	KDF Type - DER Hash Algorithm - SHA3-224, SHA3-256, SHA3-384, SHA3-512 Key Data Length - Key Data Length: 112-4096 Increment 8	SP 800-135 Rev. 1
KMAC-128	A3964	Message Length - Message Length: 0-65536 Increment 8 Key Data Length - Key Data Length: 128-1024 Increment 8	SP 800-185
KMAC-256	A3964	Message Length - Message Length: 0-65536 Increment 8 Key Data Length - Key Data Length: 128-1024 Increment 8	SP 800-185
PBKDF	A3964	Iteration Count - Iteration Count: 1000-10000 Increment 1 Password Length - Password Length: 8-128 Increment 1	SP 800-132
SHA3-224	A3964	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 202
SHA3-256	A3964	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 202
SHA3-384	A3964	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 202
SHA3-512	A3964	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 202
SHAKE-128	A3964	Output Length - Output Length: 16-65536 Increment 8	FIPS 202
SHAKE-256	A3964	Output Length - Output Length: 16-65536 Increment 8	FIPS 202
KDA OneStep SP800-56Cr2	A3965	Derived Key Length - 2048 Shared Secret Length - Shared Secret Length: 224-2048 Increment 8	SP 800-56C Rev. 2
ECDSA KeyGen (FIPS186-4)	A3966	Curve - B-233, B-283, B-409, B-571, K-233, K-283, K-409, K-571 Secret Generation Mode - Testing Candidates	FIPS 186-4
ECDSA KeyVer (FIPS186-4)	A3966	Curve - B-233, B-283, B-409, B-571, K-233, K-283, K-409, K-571	FIPS 186-4
ECDSA SigGen (FIPS186-4)	A3966	Component - No Curve - B-233, B-283, B-409, B-571, K-233, K-283, K-409, K-571 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256	FIPS 186-4
ECDSA SigVer (FIPS186-4)	A3966	Component - No Curve - B-163, B-233, B-283, B-409, B-571, K-163, K-233, K-283, K-409, K-571 Hash Algorithm - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256	FIPS 186-4
ECDSA SigGen (FIPS186-4)	A3967	Component - No Curve - B-233, B-283, B-409, B-571, K-233, K-283, K-409, K-571 Hash Algorithm - SHA3-224, SHA3-256, SHA3-384, SHA3-512	FIPS 186-4
ECDSA SigVer (FIPS186-4)	A3967	Component - No Curve - B-163, B-233, B-283, B-409, B-571, K-163, K-233, K-283, K-409, K-571 Hash Algorithm - SHA3-224, SHA3-256, SHA3-384, SHA3-512	FIPS 186-4
KAS-ECC-SSC Sp800-56Ar3	A3968	Domain Parameter Generation Methods - B-233, B-283, B-409, B-571, K-233, K-283, K-409, K-571 Scheme - ephemeralUnified - KAS Role - initiator, responder	SP 800-56A Rev. 3

Algorithm	CAVP Cert	Properties	Reference
KDA HKDF Sp800-56Cr1	A3969	Derived Key Length - 2048 Shared Secret Length - Shared Secret Length: 224-2048 Increment 8 HMAC Algorithm - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256, SHA3-224, SHA3- 256, SHA3-384	SP 800-56C Rev. 2
TLS v1.3 KDF (CVL)	A3969	HMAC Algorithm - SHA2-256, SHA2-384 KDF Running Modes - DHE, PSK, PSK-DHE	SP 800-135 Rev. 1
Counter DRBG	A3970	Prediction Resistance - No, Yes Mode - AES-128, AES-192, AES-256 Derivation Function Enabled - No, Yes	SP 800-90A Rev. 1
Hash DRBG	A3970	Prediction Resistance - No, Yes Mode - SHA-1, SHA2-256, SHA2-512	SP 800-90A Rev. 1
HMAC DRBG	A3970	Prediction Resistance - No, Yes Mode - SHA-1, SHA2-256, SHA2-512	SP 800-90A Rev. 1
AES-ECB	A3971	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
KDF SSH (CVL)	A3971	Cipher - AES-128, AES-192, AES-256 Hash Algorithm - SHA-1, SHA2-256, SHA2-384, SHA2-512	SP 800-135 Rev. 1
ECDSA SigGen (FIPS186-4)	A3972	Component - No Curve - P-224, P-256, P-384, P-521 Hash Algorithm - SHA3-224, SHA3-256, SHA3-384, SHA3-512	FIPS 186-4
ECDSA SigVer (FIPS186-4)	A3972	Component - No Curve - P-192, P-224, P-256, P-384, P-521 Hash Algorithm - SHA3-224, SHA3-256, SHA3-384, SHA3-512	FIPS 186-4
HMAC-SHA3- 224	A3972	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA3- 256	A3972	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA3- 384	A3972	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA3- 512	A3972	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
KDF ANS 9.42 (CVL)	A3972	KDF Type - DER Hash Algorithm - SHA3-224, SHA3-256, SHA3-384, SHA3-512 Key Data Length - Key Data Length: 112-4096 Increment 8	SP 800-135 Rev. 1
KMAC-128	A3972	Message Length - Message Length: 0-65536 Increment 8 Key Data Length - Key Data Length: 128-1024 Increment 8	SP 800-185
KMAC-256	A3972	Message Length - Message Length: 0-65536 Increment 8 Key Data Length - Key Data Length: 128-1024 Increment 8	SP 800-185
PBKDF	A3972	Iteration Count - Iteration Count: 1000-10000 Increment 1 Password Length - Password Length: 8-128 Increment 1	SP 800-132
SHA3-224	A3972	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 202
SHA3-256	A3972	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 202

Algorithm	CAVP Cert	Properties	Reference
SHA3-384	A3972	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 202
SHA3-512	A3972	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 202
SHAKE-128	A3972	Output Length - Output Length: 16-65536 Increment 8	FIPS 202
SHAKE-256	A3972	Output Length - Output Length: 16-65536 Increment 8	FIPS 202
AES-CBC	A3973	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CBC-CS1	A3973	Direction - decrypt, encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CBC-CS2	A3973	Direction - decrypt, encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CBC-CS3	A3973	Direction - decrypt, encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CCM	A3973	Key Length - 128, 192, 256	SP 800-38C
AES-CFB1	A3973	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CFB128	A3973	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CFB8	A3973	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CMAC	A3973	Direction - Generation, Verification Key Length - 128, 192, 256	SP 800-38B
AES-CTR	A3973	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-ECB	A3973	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-KW	A3973	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38F
AES-KWP	A3973	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38F
AES-OFB	A3973	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-XTS Testing Revision 2.0	A3973	Direction - Decrypt, Encrypt Key Length - 128, 256	SP 800-38E
AES-GCM	A3974	Direction - Decrypt, Encrypt IV Generation - External, Internal IV Generation Mode - 8.2.1 Key Length - 128, 192, 256	SP 800-38D
AES-GMAC	A3974	Direction - Decrypt, Encrypt IV Generation - External IV Generation Mode - 8.2.1 Key Length - 128, 192, 256	SP 800-38D
AES-GCM	A3975	Direction - Decrypt, Encrypt IV Generation - External, Internal	SP 800-38D

Algorithm	CAVP Cert	Properties	Reference
		IV Generation Mode - 8.2.1 Key Length - 128, 192, 256	
AES-GMAC	A3975	Direction - Decrypt, Encrypt IV Generation - External IV Generation Mode - 8.2.1 Key Length - 128, 192, 256	SP 800-38D
AES-GCM	A3976	Direction - Decrypt, Encrypt IV Generation - External, Internal IV Generation Mode - 8.2.1 Key Length - 128, 192, 256	SP 800-38D
AES-GMAC	A3976	Direction - Decrypt, Encrypt IV Generation - External IV Generation Mode - 8.2.1 Key Length - 128, 192, 256	SP 800-38D
ECDSA KeyGen (FIPS186-4)	A3977	Curve - P-224, P-256, P-384, P-521 Secret Generation Mode - Testing Candidates	FIPS 186-4
ECDSA KeyVer (FIPS186-4)	A3977	Curve - P-224, P-256, P-384, P-521	FIPS 186-4
ECDSA SigGen (FIPS186-4)	A3977	Component - No Curve - P-224, P-256, P-384, P-521 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256	FIPS 186-4
ECDSA SigVer (FIPS186-4)	A3977	Component - No Curve - P-192, P-224, P-256, P-384, P-521 Hash Algorithm - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256	FIPS 186-4
HMAC-SHA-1	A3977	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-224	A3977	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-256	A3977	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-384	A3977	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-512	A3977	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-512/224	A3977	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-512/256	A3977	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
KAS-ECC-SSC Sp800-56Ar3	A3977	Domain Parameter Generation Methods - P-224, P-256, P-384, P-521 Scheme - ephemeralUnified - KAS Role - initiator, responder	SP 800-56A Rev. 3
KDF ANS 9.42 (CVL)	A3977	KDF Type - DER Hash Algorithm - SHA-1, SHA2-224, SHA2-256, SHA2-384,	SP 800-135 Rev. 1

Algorithm	CAVP Cert	Properties	Reference
		SHA2-512, SHA2-512/224, SHA2-512/256 Key Data Length - Key Data Length: 112-4096 Increment 8	
KDF ANS 9.63 (CVL)	A3977	Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256 Key Data Length - Key Data Length: 128-4096 Increment 8	SP 800-135 Rev. 1
PBKDF	A3977	Iteration Count - Iteration Count: 1000-10000 Increment 1 Password Length - Password Length: 8-128 Increment 1	SP 800-132
RSA KeyGen (FIPS186-4)	A3977	Key Generation Mode - B.3.6 Modulo - 2048, 3072, 4096 Primality Tests - Table C.2 Private Key Format - Standard	FIPS 186-4
RSA SigGen (FIPS186-4)	A3977	Signature Type - PKCS 1.5, PKCSPSS Modulo - 2048, 3072, 4096	FIPS 186-4
RSA SigVer (FIPS186-4)	A3977	Signature Type - PKCS 1.5, PKCSPSS Modulo - 1024, 2048, 3072, 4096	FIPS 186-4
SHA-1	A3977	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 180-4
SHA2-224	A3977	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 180-4
SHA2-256	A3977	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 180-4
SHA2-384	A3977	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 180-4
SHA2-512	A3977	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 180-4
SHA2-512/224	A3977	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 180-4
SHA2-512/256	A3977	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 180-4
TLS v1.2 KDF RFC7627 (CVL)	A3977	Hash Algorithm - SHA2-256, SHA2-384, SHA2-512	SP 800-135 Rev. 1
AES-ECB	A3978	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
KDF SSH (CVL)	A3978	Cipher - AES-128, AES-192, AES-256 Hash Algorithm - SHA-1, SHA2-256, SHA2-384, SHA2-512	SP 800-135 Rev. 1
ECDSA SigGen (FIPS186-4)	A3979	Component - No Curve - P-224, P-256, P-384, P-521 Hash Algorithm - SHA3-224, SHA3-256, SHA3-384, SHA3-512	FIPS 186-4
ECDSA SigVer (FIPS186-4)	A3979	Component - No Curve - P-192, P-224, P-256, P-384, P-521 Hash Algorithm - SHA3-224, SHA3-256, SHA3-384, SHA3-512	FIPS 186-4
HMAC-SHA3-224	A3979	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA3-256	A3979	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1

Algorithm	CAVP Cert	Properties	Reference
HMAC-SHA3-384	A3979	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA3-512	A3979	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
KDF ANS 9.42 (CVL)	A3979	KDF Type - DER Hash Algorithm - SHA3-224, SHA3-256, SHA3-384, SHA3-512 Key Data Length - Key Data Length: 112-4096 Increment 8	SP 800-135 Rev. 1
KMAC-128	A3979	Message Length - Message Length: 0-65536 Increment 8 Key Data Length - Key Data Length: 128-1024 Increment 8	SP 800-185
KMAC-256	A3979	Message Length - Message Length: 0-65536 Increment 8 Key Data Length - Key Data Length: 128-1024 Increment 8	SP 800-185
PBKDF	A3979	Iteration Count - Iteration Count: 1000-10000 Increment 1 Password Length - Password Length: 8-128 Increment 1	SP 800-132
SHA3-224	A3979	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 202
SHA3-256	A3979	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 202
SHA3-384	A3979	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 202
SHA3-512	A3979	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 202
SHAKE-128	A3979	Output Length - Output Length: 16-65536 Increment 8	FIPS 202
SHAKE-256	A3979	Output Length - Output Length: 16-65536 Increment 8	FIPS 202
AES-CBC	A3980	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CBC-CS1	A3980	Direction - decrypt, encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CBC-CS2	A3980	Direction - decrypt, encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CBC-CS3	A3980	Direction - decrypt, encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CCM	A3980	Key Length - 128, 192, 256	SP 800-38C
AES-CFB1	A3980	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CFB128	A3980	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CFB8	A3980	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CMAC	A3980	Direction - Generation, Verification Key Length - 128, 192, 256	SP 800-38B
AES-CTR	A3980	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-ECB	A3980	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A

Algorithm	CAVP Cert	Properties	Reference
AES-KW	A3980	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38F
AES-KWP	A3980	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38F
AES-OFB	A3980	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-XTS Testing Revision 2.0	A3980	Direction - Decrypt, Encrypt Key Length - 128, 256	SP 800-38E
AES-CBC	A3981	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CBC-CS1	A3981	Direction - decrypt, encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CBC-CS2	A3981	Direction - decrypt, encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CBC-CS3	A3981	Direction - decrypt, encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CCM	A3981	Key Length - 128, 192, 256	SP 800-38C
AES-CFB1	A3981	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CFB128	A3981	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CFB8	A3981	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CMAC	A3981	Direction - Generation, Verification Key Length - 128, 192, 256	SP 800-38B
AES-CTR	A3981	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-ECB	A3981	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-KW	A3981	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38F
AES-KWP	A3981	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38F
AES-OFB	A3981	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-XTS Testing Revision 2.0	A3981	Direction - Decrypt, Encrypt Key Length - 128, 256	SP 800-38E
AES-CBC	A3982	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CBC-CS1	A3982	Direction - decrypt, encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CBC-CS2	A3982	Direction - decrypt, encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CBC-CS3	A3982	Direction - decrypt, encrypt Key Length - 128, 192, 256	SP 800-38A

Algorithm	CAVP Cert	Properties	Reference
AES-CCM	A3982	Key Length - 128, 192, 256	SP 800-38C
AES-CFB1	A3982	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CFB128	A3982	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CFB8	A3982	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CMAC	A3982	Direction - Generation, Verification Key Length - 128, 192, 256	SP 800-38B
AES-CTR	A3982	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-ECB	A3982	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-KW	A3982	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38F
AES-KWP	A3982	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38F
AES-OFB	A3982	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-XTS Testing Revision 2.0	A3982	Direction - Decrypt, Encrypt Key Length - 128, 256	SP 800-38E
ECDSA KeyGen (FIPS186-4)	A3983	Curve - P-224, P-256, P-384, P-521 Secret Generation Mode - Testing Candidates	FIPS 186-4
ECDSA KeyVer (FIPS186-4)	A3983	Curve - P-224, P-256, P-384, P-521	FIPS 186-4
ECDSA SigGen (FIPS186-4)	A3983	Component - No Curve - P-224, P-256, P-384, P-521 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256	FIPS 186-4
ECDSA SigVer (FIPS186-4)	A3983	Component - No Curve - P-192, P-224, P-256, P-384, P-521 Hash Algorithm - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256	FIPS 186-4
HMAC-SHA-1	A3983	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2- 224	A3983	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2- 256	A3983	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2- 384	A3983	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2- 512	A3983	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2- 512/224	A3983	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1

Algorithm	CAVP Cert	Properties	Reference
HMAC-SHA2-512/256	A3983	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
KAS-ECC-SSC Sp800-56Ar3	A3983	Domain Parameter Generation Methods - P-224, P-256, P-384, P-521 Scheme - ephemeralUnified - KAS Role - initiator, responder	SP 800-56A Rev. 3
KDF ANS 9.42 (CVL)	A3983	KDF Type - DER Hash Algorithm - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256 Key Data Length - Key Data Length: 112-4096 Increment 8	SP 800-135 Rev. 1
KDF ANS 9.63 (CVL)	A3983	Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256 Key Data Length - Key Data Length: 128-4096 Increment 8	SP 800-135 Rev. 1
PBKDF	A3983	Iteration Count - Iteration Count: 1000-10000 Increment 1 Password Length - Password Length: 8-128 Increment 1	SP 800-132
RSA KeyGen (FIPS186-4)	A3983	Key Generation Mode - B.3.6 Modulo - 2048, 3072, 4096 Primality Tests - Table C.2 Private Key Format - Standard	FIPS 186-4
RSA SigGen (FIPS186-4)	A3983	Signature Type - PKCS 1.5, PKCSPSS Modulo - 2048, 3072, 4096	FIPS 186-4
RSA SigVer (FIPS186-4)	A3983	Signature Type - PKCS 1.5, PKCSPSS Modulo - 1024, 2048, 3072, 4096	FIPS 186-4
SHA-1	A3983	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 180-4
SHA2-224	A3983	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 180-4
SHA2-256	A3983	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 180-4
SHA2-384	A3983	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 180-4
SHA2-512	A3983	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 180-4
SHA2-512/224	A3983	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 180-4
SHA2-512/256	A3983	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 180-4
TLS v1.2 KDF RFC7627 (CVL)	A3983	Hash Algorithm - SHA2-256, SHA2-384, SHA2-512	SP 800-135 Rev. 1
AES-ECB	A3984	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
KDF SSH (CVL)	A3984	Cipher - AES-128, AES-192, AES-256 Hash Algorithm - SHA-1, SHA2-256, SHA2-384, SHA2-512	SP 800-135 Rev. 1
AES-ECB	A3985	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A

Algorithm	CAVP Cert	Properties	Reference
KDF SSH (CVL)	A3985	Cipher - AES-128, AES-192, AES-256 Hash Algorithm - SHA-1, SHA2-256, SHA2-384, SHA2-512	SP 800-135 Rev. 1
AES-ECB	A3986	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
KDF SSH (CVL)	A3986	Cipher - AES-128, AES-192, AES-256 Hash Algorithm - SHA-1, SHA2-256, SHA2-384, SHA2-512	SP 800-135 Rev. 1
AES-ECB	A3987	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
KDF SSH (CVL)	A3987	Cipher - AES-128, AES-192, AES-256 Hash Algorithm - SHA-1, SHA2-256, SHA2-384, SHA2-512	SP 800-135 Rev. 1
AES-GCM	A3988	Direction - Decrypt, Encrypt IV Generation - External, Internal IV Generation Mode - 8.2.1 Key Length - 128, 192, 256	SP 800-38D
AES-GMAC	A3988	Direction - Decrypt, Encrypt IV Generation - External IV Generation Mode - 8.2.1 Key Length - 128, 192, 256	SP 800-38D
AES-GCM	A3989	Direction - Decrypt, Encrypt IV Generation - External, Internal IV Generation Mode - 8.2.1 Key Length - 128, 192, 256	SP 800-38D
AES-GMAC	A3989	Direction - Decrypt, Encrypt IV Generation - External IV Generation Mode - 8.2.1 Key Length - 128, 192, 256	SP 800-38D
AES-GCM	A3990	Direction - Decrypt, Encrypt IV Generation - External, Internal IV Generation Mode - 8.2.1 Key Length - 128, 192, 256	SP 800-38D
AES-GMAC	A3990	Direction - Decrypt, Encrypt IV Generation - External IV Generation Mode - 8.2.1 Key Length - 128, 192, 256	SP 800-38D
KDF SP800-108	A3991	KDF Mode - Counter, Feedback Supported Lengths - Supported Lengths: 112-4096 Increment 8	SP 800-108 Rev. 1
KAS-FFC-SSC Sp800-56Ar3	A3992	Domain Parameter Generation Methods - ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192, MODP-2048, MODP-3072, MODP-4096, MODP-6144, MODP-8192 Scheme - dhEphem - KAS Role - initiator, responder	SP 800-56A Rev. 3
Safe Primes Key Generation	A3992	Safe Prime Groups - ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192, MODP-2048, MODP-3072, MODP-4096, MODP-6144, MODP-8192	SP 800-56A Rev. 3

Algorithm	CAVP Cert	Properties	Reference
Safe Primes Key Verification	A3992	Safe Prime Groups - ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192, MODP-2048, MODP-3072, MODP-4096, MODP-6144, MODP-8192	SP 800-56A Rev. 3
ECDSA KeyGen (FIPS186-4)	A3993	Curve - P-224, P-256, P-384, P-521 Secret Generation Mode - Testing Candidates	FIPS 186-4
ECDSA KeyVer (FIPS186-4)	A3993	Curve - P-224, P-256, P-384, P-521	FIPS 186-4
ECDSA SigGen (FIPS186-4)	A3993	Component - No Curve - P-224, P-256, P-384, P-521 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256	FIPS 186-4
ECDSA SigVer (FIPS186-4)	A3993	Component - No Curve - P-192, P-224, P-256, P-384, P-521 Hash Algorithm - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256	FIPS 186-4
HMAC-SHA-1	A3993	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-224	A3993	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-256	A3993	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-384	A3993	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-512	A3993	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-512/224	A3993	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-512/256	A3993	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
KAS-ECC-SSC Sp800-56Ar3	A3993	Domain Parameter Generation Methods - P-224, P-256, P-384, P-521 Scheme - ephemeralUnified - KAS Role - initiator, responder	SP 800-56A Rev. 3
KDF ANS 9.42 (CVL)	A3993	KDF Type - DER Hash Algorithm - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256 Key Data Length - Key Data Length: 112-4096 Increment 8	SP 800-135 Rev. 1
KDF ANS 9.63 (CVL)	A3993	Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256 Key Data Length - Key Data Length: 128-4096 Increment 8	SP 800-135 Rev. 1
PBKDF	A3993	Iteration Count - Iteration Count: 1000-10000 Increment 1 Password Length - Password Length: 8-128 Increment 1	SP 800-132
RSA KeyGen (FIPS186-4)	A3993	Key Generation Mode - B.3.6 Modulo - 2048, 3072, 4096 Primality Tests - Table C.2 Private Key Format - Standard	FIPS 186-4

Algorithm	CAVP Cert	Properties	Reference
RSA SigGen (FIPS186-4)	A3993	Signature Type - PKCS 1.5, PKCSPSS Modulo - 2048, 3072, 4096	FIPS 186-4
RSA SigVer (FIPS186-4)	A3993	Signature Type - PKCS 1.5, PKCSPSS Modulo - 1024, 2048, 3072, 4096	FIPS 186-4
SHA-1	A3993	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 180-4
SHA2-224	A3993	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 180-4
SHA2-256	A3993	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 180-4
SHA2-384	A3993	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 180-4
SHA2-512	A3993	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 180-4
SHA2-512/224	A3993	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 180-4
SHA2-512/256	A3993	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 180-4
TLS v1.2 KDF RFC7627 (CVL)	A3993	Hash Algorithm - SHA2-256, SHA2-384, SHA2-512	SP 800-135 Rev. 1
AES-GCM	A3994	Direction - Decrypt, Encrypt IV Generation - External, Internal IV Generation Mode - 8.2.1 Key Length - 128, 192, 256	SP 800-38D
AES-GMAC	A3994	Direction - Decrypt, Encrypt IV Generation - External IV Generation Mode - 8.2.1 Key Length - 128, 192, 256	SP 800-38D
AES-GCM	A3995	Direction - Decrypt, Encrypt IV Generation - External, Internal IV Generation Mode - 8.2.1 Key Length - 128, 192, 256	SP 800-38D
AES-GMAC	A3995	Direction - Decrypt, Encrypt IV Generation - External IV Generation Mode - 8.2.1 Key Length - 128, 192, 256	SP 800-38D
AES-GCM	A3996	Direction - Decrypt, Encrypt IV Generation - External, Internal IV Generation Mode - 8.2.1 Key Length - 128, 192, 256	SP 800-38D
AES-GMAC	A3996	Direction - Decrypt, Encrypt IV Generation - External IV Generation Mode - 8.2.1 Key Length - 128, 192, 256	SP 800-38D
AES-GCM	A3997	Direction - Decrypt, Encrypt IV Generation - External, Internal	SP 800-38D

Algorithm	CAVP Cert	Properties	Reference
		IV Generation Mode - 8.2.1 Key Length - 128, 192, 256	
AES-GMAC	A3997	Direction - Decrypt, Encrypt IV Generation - External IV Generation Mode - 8.2.1 Key Length - 128, 192, 256	SP 800-38D
AES-GCM	A3998	Direction - Decrypt, Encrypt IV Generation - External, Internal IV Generation Mode - 8.2.1 Key Length - 128, 192, 256	SP 800-38D
AES-GMAC	A3998	Direction - Decrypt, Encrypt IV Generation - External IV Generation Mode - 8.2.1 Key Length - 128, 192, 256	SP 800-38D
AES-GCM	A3999	Direction - Decrypt, Encrypt IV Generation - External, Internal IV Generation Mode - 8.2.1 Key Length - 128, 192, 256	SP 800-38D
AES-GMAC	A3999	Direction - Decrypt, Encrypt IV Generation - External IV Generation Mode - 8.2.1 Key Length - 128, 192, 256	SP 800-38D
AES-GCM	A4000	Direction - Decrypt, Encrypt IV Generation - External, Internal IV Generation Mode - 8.2.1 Key Length - 128, 192, 256	SP 800-38D
AES-GMAC	A4000	Direction - Decrypt, Encrypt IV Generation - External IV Generation Mode - 8.2.1 Key Length - 128, 192, 256	SP 800-38D
AES-GCM	A4001	Direction - Decrypt, Encrypt IV Generation - External, Internal IV Generation Mode - 8.2.1 Key Length - 128, 192, 256	SP 800-38D
AES-GMAC	A4001	Direction - Decrypt, Encrypt IV Generation - External IV Generation Mode - 8.2.1 Key Length - 128, 192, 256	SP 800-38D
AES-GCM	A4002	Direction - Decrypt, Encrypt IV Generation - External, Internal IV Generation Mode - 8.2.1 Key Length - 128, 192, 256	SP 800-38D
AES-GMAC	A4002	Direction - Decrypt, Encrypt IV Generation - External IV Generation Mode - 8.2.1 Key Length - 128, 192, 256	SP 800-38D
ECDSA KeyGen (FIPS186-4)	A4003	Curve - P-224, P-256, P-384, P-521 Secret Generation Mode - Testing Candidates	FIPS 186-4

Algorithm	CAVP Cert	Properties	Reference
ECDSA KeyVer (FIPS186-4)	A4003	Curve - P-224, P-256, P-384, P-521	FIPS 186-4
ECDSA SigGen (FIPS186-4)	A4003	Component - No Curve - P-224, P-256, P-384, P-521 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256	FIPS 186-4
ECDSA SigVer (FIPS186-4)	A4003	Component - No Curve - P-192, P-224, P-256, P-384, P-521 Hash Algorithm - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256	FIPS 186-4
HMAC-SHA-1	A4003	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-224	A4003	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-256	A4003	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-384	A4003	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-512	A4003	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-512/224	A4003	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-512/256	A4003	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
KAS-ECC-SSC Sp800-56Ar3	A4003	Domain Parameter Generation Methods - P-224, P-256, P-384, P-521 Scheme - ephemeralUnified - KAS Role - initiator, responder	SP 800-56A Rev. 3
KDF ANS 9.42 (CVL)	A4003	KDF Type - DER Hash Algorithm - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256 Key Data Length - Key Data Length: 112-4096 Increment 8	SP 800-135 Rev. 1
KDF ANS 9.63 (CVL)	A4003	Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256 Key Data Length - Key Data Length: 128-4096 Increment 8	SP 800-135 Rev. 1
PBKDF	A4003	Iteration Count - Iteration Count: 1000-10000 Increment 1 Password Length - Password Length: 8-128 Increment 1	SP 800-132
RSA KeyGen (FIPS186-4)	A4003	Key Generation Mode - B.3.6 Modulo - 2048, 3072, 4096 Primality Tests - Table C.2 Private Key Format - Standard	FIPS 186-4
RSA SigGen (FIPS186-4)	A4003	Signature Type - PKCS 1.5, PKCSPSS Modulo - 2048, 3072, 4096	FIPS 186-4
RSA SigVer (FIPS186-4)	A4003	Signature Type - PKCS 1.5, PKCSPSS Modulo - 1024, 2048, 3072, 4096	FIPS 186-4
SHA-1	A4003	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 180-4

Algorithm	CAVP Cert	Properties	Reference
SHA2-224	A4003	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 180-4
SHA2-256	A4003	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 180-4
SHA2-384	A4003	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 180-4
SHA2-512	A4003	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 180-4
SHA2-512/224	A4003	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 180-4
SHA2-512/256	A4003	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 180-4
TLS v1.2 KDF RFC7627 (CVL)	A4003	Hash Algorithm - SHA2-256, SHA2-384, SHA2-512	SP 800-135 Rev. 1
ECDSA KeyGen (FIPS186-4)	A4004	Curve - P-224, P-256, P-384, P-521 Secret Generation Mode - Testing Candidates	FIPS 186-4
ECDSA KeyVer (FIPS186-4)	A4004	Curve - P-224, P-256, P-384, P-521	FIPS 186-4
ECDSA SigGen (FIPS186-4)	A4004	Component - No Curve - P-224, P-256, P-384, P-521 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256	FIPS 186-4
ECDSA SigVer (FIPS186-4)	A4004	Component - No Curve - P-192, P-224, P-256, P-384, P-521 Hash Algorithm - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256	FIPS 186-4
HMAC-SHA-1	A4004	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2- 224	A4004	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2- 256	A4004	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2- 384	A4004	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2- 512	A4004	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2- 512/224	A4004	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2- 512/256	A4004	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
KAS-ECC-SSC Sp800-56Ar3	A4004	Domain Parameter Generation Methods - P-224, P-256, P-384, P-521 Scheme - ephemeralUnified - KAS Role - initiator, responder	SP 800-56A Rev. 3
KDF ANS 9.42 (CVL)	A4004	KDF Type - DER Hash Algorithm - SHA-1, SHA2-224, SHA2-256, SHA2-384,	SP 800-135 Rev. 1

Algorithm	CAVP Cert	Properties	Reference
		SHA2-512, SHA2-512/224, SHA2-512/256 Key Data Length - Key Data Length: 112-4096 Increment 8	
KDF ANS 9.63 (CVL)	A4004	Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256 Key Data Length - Key Data Length: 128-4096 Increment 8	SP 800-135 Rev. 1
PBKDF	A4004	Iteration Count - Iteration Count: 1000-10000 Increment 1 Password Length - Password Length: 8-128 Increment 1	SP 800-132
RSA KeyGen (FIPS186-4)	A4004	Key Generation Mode - B.3.6 Modulo - 2048, 3072, 4096 Primality Tests - Table C.2 Private Key Format - Standard	FIPS 186-4
RSA SigGen (FIPS186-4)	A4004	Signature Type - PKCS 1.5, PKCSPSS Modulo - 2048, 3072, 4096	FIPS 186-4
RSA SigVer (FIPS186-4)	A4004	Signature Type - PKCS 1.5, PKCSPSS Modulo - 1024, 2048, 3072, 4096	FIPS 186-4
SHA-1	A4004	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 180-4
SHA2-224	A4004	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 180-4
SHA2-256	A4004	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 180-4
SHA2-384	A4004	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 180-4
SHA2-512	A4004	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 180-4
SHA2-512/224	A4004	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 180-4
SHA2-512/256	A4004	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 180-4
TLS v1.2 KDF RFC7627 (CVL)	A4004	Hash Algorithm - SHA2-256, SHA2-384, SHA2-512	SP 800-135 Rev. 1
ECDSA KeyGen (FIPS186-4)	A4005	Curve - P-224, P-256, P-384, P-521 Secret Generation Mode - Testing Candidates	FIPS 186-4
ECDSA KeyVer (FIPS186-4)	A4005	Curve - P-224, P-256, P-384, P-521	FIPS 186-4
ECDSA SigGen (FIPS186-4)	A4005	Component - No Curve - P-224, P-256, P-384, P-521 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256	FIPS 186-4
ECDSA SigVer (FIPS186-4)	A4005	Component - No Curve - P-192, P-224, P-256, P-384, P-521 Hash Algorithm - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256	FIPS 186-4
HMAC-SHA-1	A4005	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-224	A4005	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1

Algorithm	CAVP Cert	Properties	Reference
HMAC-SHA2-256	A4005	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-384	A4005	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-512	A4005	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-512/224	A4005	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-512/256	A4005	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
KAS-ECC-SSC Sp800-56Ar3	A4005	Domain Parameter Generation Methods - P-224, P-256, P-384, P-521 Scheme - ephemeralUnified - KAS Role - initiator, responder	SP 800-56A Rev. 3
KDF ANS 9.42 (CVL)	A4005	KDF Type - DER Hash Algorithm - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256 Key Data Length - Key Data Length: 112-4096 Increment 8	SP 800-135 Rev. 1
KDF ANS 9.63 (CVL)	A4005	Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256 Key Data Length - Key Data Length: 128-4096 Increment 8	SP 800-135 Rev. 1
PBKDF	A4005	Iteration Count - Iteration Count: 1000-10000 Increment 1 Password Length - Password Length: 8-128 Increment 1	SP 800-132
RSA KeyGen (FIPS186-4)	A4005	Key Generation Mode - B.3.6 Modulo - 2048, 3072, 4096 Primality Tests - Table C.2 Private Key Format - Standard	FIPS 186-4
RSA SigGen (FIPS186-4)	A4005	Signature Type - PKCS 1.5, PKCSPSS Modulo - 2048, 3072, 4096	FIPS 186-4
RSA SigVer (FIPS186-4)	A4005	Signature Type - PKCS 1.5, PKCSPSS Modulo - 1024, 2048, 3072, 4096	FIPS 186-4
SHA-1	A4005	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 180-4
SHA2-224	A4005	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 180-4
SHA2-256	A4005	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 180-4
SHA2-384	A4005	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 180-4
SHA2-512	A4005	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 180-4
SHA2-512/224	A4005	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 180-4
SHA2-512/256	A4005	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 180-4

Algorithm	CAVP Cert	Properties	Reference
TLS v1.2 KDF RFC7627 (CVL)	A4005	Hash Algorithm - SHA2-256, SHA2-384, SHA2-512	SP 800-135 Rev. 1

Table 5: Approved Algorithms

The table above lists all implemented modes or methods of operation for the approved cryptographic algorithms of the module that are employed for approved services (Approved Services table).

Vendor-Affirmed Algorithms:

Name	Properties	Implementation	Reference
Cryptographic Key Generation (CKG)	Key Type:Asymmetric RSA:2048, 3072, 4096-bit keys ECDSA:P-224, P-256, P-384, P-521, B-233, B-283, B-409, B-571, K-233, K-283, K-409, K-571 elliptic curves Safe Prime Groups:ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192, MODP-2048, MODP-3072, MODP-4096, MODP-6144, MODP-8192	N/A	SP800-133rev2, Section 4, example 1

Table 6: Vendor-Affirmed Algorithms

Non-Approved, Allowed Algorithms:

N/A for this module.

Non-Approved, Allowed Algorithms with No Security Claimed:

N/A for this module.

Non-Approved, Not Allowed Algorithms:

Name	Use and Function
AES GCM (external IV)	Encryption
DSA	Signature generation
DSA	Signature verification
DSA	Key pair generation
DSA	Key pair verification
ECDSA with curve P-192	Key pair generation
RSA and ECDSA (pre-hashed message)	Signature generation (pre-hashed message)
RSA and ECDSA (pre-hashed message)	Signature verification (pre-hashed message)
RSA X9.31	Signature generation
RSA X9.31	Signature verification
RSA primitive	Asymmetric encryption
RSA primitive	Asymmetric decryption
RSA-OAEP	Asymmetric encryption
RSA-OAEP	Asymmetric decryption
RSASVE	Secret value encapsulation

Name	Use and Function
RSASVE	Secret value decapsulation

Table 7: Non-Approved, Not Allowed Algorithms

The table above lists all the non-approved cryptographic algorithms of the module employed by the non-approved services in the Non-Approved Services table.

2.6 Security Function Implementations

[illegible]

Name	Type	Description	Properties	Algorithms
				AES-CFB128
				AES-CFB128
				AES-CFB128
				AES-CFB128
				AES-CFB128
				AES-CFB128
				AES-CFB8
				AES-CFB8
				AES-CFB8
				AES-CFB8
				AES-CFB8
				AES-CFB8
				AES-CFB8
				AES-CTR
				AES-CTR
				AES-CTR
				AES-CTR
				AES-CTR
				AES-CTR
				AES-CTR
				AES-CTR
				AES-ECB
				AES-ECB
				AES-ECB
				AES-ECB
				AES-ECB
				AES-ECB
				AES-ECB
				AES-ECB
				AES-ECB
				AES-ECB
				AES-ECB
				AES-ECB
				AES-ECB
				AES-ECB
				AES-OFB
				AES-OFB
				AES-OFB
				AES-OFB
				AES-OFB
				AES-OFB
				AES-OFB
				AES-XTS Testing
				Revision 2.0
				AES-XTS Testing
				Revision 2.0
				AES-XTS Testing
				Revision 2.0
				AES-XTS Testing
				Revision 2.0
				AES-XTS Testing
				Revision 2.0
				AES-XTS Testing
				Revision 2.0
				AES-XTS Testing

Name	Type	Description	Properties	Algorithms
				Revision 2.0 AES-GCM AES-GCM AES-GCM AES-GCM AES-GCM AES-GCM AES-GCM AES-GCM AES-GCM AES-GCM AES-GCM AES-GCM AES-GCM AES-GCM AES-GCM AES-GCM
Symmetric decryption	BC-UnAuth BC-Auth	Symmetric decryption	AES-CBC:128, 192, 256 bits AES-CBC-CS1:128, 192, 256 bits AES-CBC-CS2:128, 192, 256 bits AES-CBC-CS3:128, 192, 256 bits AES-CCM:128, 192, 256 bits AES-CFB1:128, 192, 256 bits AES-CFB128:128, 192, 256 bits AES-CFB8:128, 192, 256 bits AES-CTR:128, 192, 256 bits AES-ECB:128, 192, 256 bits AES-OFB:128, 192, 256 bits AES-XTS Testing Revision 2.0:128, 256 bits AES-GCM:128, 192, 256 bits	AES-CBC AES-CBC AES-CBC AES-CBC AES-CBC AES-CBC AES-CBC-CS1 AES-CBC-CS1 AES-CBC-CS1 AES-CBC-CS1 AES-CBC-CS1 AES-CBC-CS1 AES-CBC-CS1 AES-CBC-CS2 AES-CBC-CS2 AES-CBC-CS2 AES-CBC-CS2 AES-CBC-CS2 AES-CBC-CS2 AES-CBC-CS2 AES-CBC-CS2 AES-CBC-CS3 AES-CBC-CS3 AES-CBC-CS3 AES-CBC-CS3 AES-CBC-CS3 AES-CBC-CS3 AES-CBC-CS3 AES-CCM AES-CCM AES-CCM AES-CCM AES-CCM AES-CCM AES-CCM

Name	Type	Description	Properties	Algorithms
				AES-CFB1 AES-CFB1 AES-CFB1 AES-CFB1 AES-CFB1 AES-CFB1 AES-CFB1 AES-CFB128 AES-CFB128 AES-CFB128 AES-CFB128 AES-CFB128 AES-CFB128 AES-CFB128 AES-CFB8 AES-CFB8 AES-CFB8 AES-CFB8 AES-CFB8 AES-CFB8 AES-CFB8 AES-CTR AES-CTR AES-CTR AES-CTR AES-CTR AES-CTR AES-CTR AES-CTR AES-CTR AES-CTR AES-ECB AES-ECB AES-ECB AES-ECB AES-ECB AES-ECB AES-ECB AES-ECB AES-ECB AES-ECB AES-ECB AES-OFB AES-OFB AES-OFB AES-OFB AES-OFB AES-OFB AES-OFB AES-XTS Testing Revision 2.0 AES-XTS Testing Revision 2.0 AES-XTS Testing

Name	Type	Description	Properties	Algorithms
				Revision 2.0 AES-XTS Testing Revision 2.0 AES-XTS Testing Revision 2.0 AES-XTS Testing Revision 2.0 AES-XTS Testing Revision 2.0 AES-GCM AES-GCM AES-GCM AES-GCM AES-GCM AES-GCM AES-GCM AES-GCM AES-GCM AES-GCM AES-GCM AES-GCM AES-GCM AES-GCM AES-GCM AES-GCM
Key wrapping	KTS-Wrap	Key wrapping (compliant with IG D.G)	AES-KW:128, 192, 256 bits AES-KWP:128, 192, 256 bits	AES-KW AES-KW AES-KW AES-KW AES-KW AES-KW AES-KWP AES-KWP AES-KWP AES-KWP AES-KWP AES-KWP AES-KWP
Key unwrapping	KTS-Wrap	Key unwrapping (compliant with IG D.G)	AES-KW:128, 192, 256 bits AES-KWP:128, 192, 256 bits	AES-KW AES-KW AES-KW AES-KW AES-KW AES-KW AES-KWP AES-KWP AES-KWP AES-KWP AES-KWP

Name	Type	Description	Properties	Algorithms
				AES-KWP AES-KWP
Key pair generation	AsymKeyPair- KeyGen	Key pair generation	ECDSA KeyGen (FIPS186-4):P-224, P-256, P-384, P-521, K-233, K-283, K-409, K-571, B-233, B-283, B-409, B-571 (112, 128, 192, 256 bits) RSA KeyGen (FIPS186-4):2048-15360 bits (112-256 bits) Safe Primes Key Generation:MODP-2048, MODP-3072, MODP-4096, MODP-6144, MODP-8192, ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192 (112-200 bits)	ECDSA KeyGen (FIPS186-4) ECDSA KeyGen (FIPS186-4) ECDSA KeyGen (FIPS186-4) ECDSA KeyGen (FIPS186-4) ECDSA KeyGen (FIPS186-4) ECDSA KeyGen (FIPS186-4) ECDSA KeyGen (FIPS186-4) ECDSA KeyGen (FIPS186-4) ECDSA KeyGen (FIPS186-4) RSA KeyGen (FIPS186-4) RSA KeyGen (FIPS186-4) RSA KeyGen (FIPS186-4) RSA KeyGen (FIPS186-4) RSA KeyGen (FIPS186-4) RSA KeyGen (FIPS186-4) RSA KeyGen (FIPS186-4) Safe Primes Key Generation
Key pair verification	AsymKeyPair- KeyVer	Key pair verification	ECDSA KeyVer (FIPS186-4):P-192, P-224, P-256, P-384, P-521, K-163, K-233, K-283, K-409, K-571, B-163, B-233, B-283, B-409, B-571 (80-256 bits) Safe Primes Key Verification:MODP-2048, MODP-3072, MODP-4096, MODP-6144, MODP-8192, ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144,	ECDSA KeyVer (FIPS186-4) ECDSA KeyVer (FIPS186-4) ECDSA KeyVer (FIPS186-4) ECDSA KeyVer (FIPS186-4) ECDSA KeyVer (FIPS186-4) ECDSA KeyVer (FIPS186-4) ECDSA KeyVer (FIPS186-4) ECDSA KeyVer (FIPS186-4) ECDSA KeyVer (FIPS186-4) ECDSA KeyVer (FIPS186-4) ECDSA KeyVer (FIPS186-4) ECDSA KeyVer (FIPS186-4) ECDSA KeyVer (FIPS186-4) ECDSA KeyVer (FIPS186-4) ECDSA KeyVer (FIPS186-4) ECDSA KeyVer (FIPS186-4) ECDSA KeyVer (FIPS186-4) Safe Primes Key Verification

[illegible]

Name	Type	Description	Properties	Algorithms
				RSA SigVer (FIPS186-4) ECDSA SigVer (FIPS186-4) ECDSA SigVer (FIPS186-4) ECDSA SigVer (FIPS186-4) ECDSA SigVer (FIPS186-4) ECDSA SigVer (FIPS186-4) ECDSA SigVer (FIPS186-4) ECDSA SigVer (FIPS186-4) ECDSA SigVer (FIPS186-4) ECDSA SigVer (FIPS186-4) ECDSA SigVer (FIPS186-4) ECDSA SigVer (FIPS186-4) ECDSA SigVer (FIPS186-4) ECDSA SigVer (FIPS186-4)
Message authentication	MAC	Message authentication	AES-CMAC:128, 192, 256 bits AES-GMAC:128, 192, 256 bits HMAC-SHA-1:112-524288 bits (112-256 bits) HMAC-SHA2-224:112-524288 bits (112-256 bits) HMAC-SHA2-256:112-524288 bits (112-256 bits) HMAC-SHA2-384:112-524288 bits (112-256 bits) HMAC-SHA2-512:112-524288 bits (112-256 bits) HMAC-SHA2-512/224:112-524288 bits (112-256 bits) HMAC-SHA2-512/256:112-524288 bits (112-	AES-CMAC AES-CMAC AES-CMAC AES-CMAC AES-CMAC AES-GMAC AES-GMAC AES-GMAC AES-GMAC AES-GMAC AES-GMAC AES-GMAC AES-GMAC AES-GMAC AES-GMAC AES-GMAC AES-GMAC HMAC-SHA-1 HMAC-SHA-1 HMAC-SHA-1

Name	Type	Description	Properties	Algorithms
			256 bits)	HMAC-SHA-1
			HMAC-SHA3-	HMAC-SHA-1
			224:112-524288	HMAC-SHA-1
			bits (112-256 bits)	HMAC-SHA-1
			HMAC-SHA3-	HMAC-SHA2-224
			256:112-524288	HMAC-SHA2-224
			bits (112-256 bits)	HMAC-SHA2-224
			HMAC-SHA3-	HMAC-SHA2-224
			384:112-524288	HMAC-SHA2-224
			bits (112-256 bits)	HMAC-SHA2-224
			HMAC-SHA3-	HMAC-SHA2-224
			512:112-524288	HMAC-SHA2-256
			bits (112-256 bits)	HMAC-SHA2-256
			KMAC-128:128-	HMAC-SHA2-256
			1024 bits (128-256	HMAC-SHA2-256
			bits)	HMAC-SHA2-256
			KMAC-256:128-	HMAC-SHA2-256
			1024 bits (128-256	HMAC-SHA2-256
			bits)	HMAC-SHA2-256
				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-SHA2-512/224
				HMAC-SHA2-512/224
				HMAC-SHA2-512/224
				HMAC-SHA2-512/224
				HMAC-SHA2-512/224
				HMAC-SHA2-512/224
				HMAC-SHA2-512/224
				HMAC-SHA2-512/224
				HMAC-SHA2-512/256
				HMAC-SHA2-512/256
				HMAC-SHA2-512/256

Name	Type	Description	Properties	Algorithms
				HMAC-SHA2-512/256 HMAC-SHA2-512/256 HMAC-SHA2-512/256 HMAC-SHA2-512/256 HMAC-SHA3-224 HMAC-SHA3-224 HMAC-SHA3-224 HMAC-SHA3-256 HMAC-SHA3-256 HMAC-SHA3-256 HMAC-SHA3-384 HMAC-SHA3-384 HMAC-SHA3-384 HMAC-SHA3-512 HMAC-SHA3-512 HMAC-SHA3-512 KMAC-128 KMAC-128 KMAC-128 KMAC-256 KMAC-256 KMAC-256
Shared secret computation	KAS-SSC	Shared secret computation	KAS-FFC-SSC Sp800-56Ar3:MODP-2048, MODP-3072, MODP-4096, MODP-6144, MODP-8192, ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192 (112-200 bits) KAS-ECC-SSC Sp800-56Ar3:P-224, P-256, P-384, P-521, K-233, K-283, K-409, K-571, B-233, B-283, B-409, B-571 (112, 128, 192, 256 bits)	KAS-FFC-SSC Sp800-56Ar3 KAS-ECC-SSC Sp800-56Ar3 KAS-ECC-SSC Sp800-56Ar3 KAS-ECC-SSC Sp800-56Ar3 KAS-ECC-SSC Sp800-56Ar3 KAS-ECC-SSC Sp800-56Ar3 KAS-ECC-SSC Sp800-56Ar3 KAS-ECC-SSC Sp800-56Ar3 KAS-ECC-SSC Sp800-56Ar3
Key derivation	KAS-135KDF KAS-56CKDF KBKDF	Key derivation	KDF ANS 9.42:112-4096 bits (112-256 bits) KDF ANS 9.63:128-4096 bits (128-256 bits)	KDF ANS 9.42 KDF ANS 9.42 KDF ANS 9.42 KDF ANS 9.42 KDF ANS 9.42

Name	Type	Description	Properties	Algorithms
			bits) TLS v1.2 KDF RFC7627:TLS derived secret (112- 256 bits) KDA OneStep SP800- 56Cr2:Shared secret (224-2048 bits) KDA HKDF Sp800- 56Cr1:224-2048 bits (112-256 bits) TLS v1.3 KDF:TLS derived secret (112- 256 bits) KDF SSH:112-256 bits KDF SP800- 108:112-4096 bits (112-256 bits)	KDF ANS 9.42 KDF ANS 9.42 KDF ANS 9.42 KDF ANS 9.42 KDF ANS 9.42 KDF ANS 9.63 KDF ANS 9.63 KDF ANS 9.63 KDF ANS 9.63 KDF ANS 9.63 KDF ANS 9.63 KDF ANS 9.63 TLS v1.2 KDF RFC7627 TLS v1.2 KDF RFC7627 TLS v1.2 KDF RFC7627 TLS v1.2 KDF RFC7627 TLS v1.2 KDF RFC7627 TLS v1.2 KDF RFC7627 TLS v1.2 KDF RFC7627 KDA OneStep SP800-56Cr2 KDA HKDF Sp800- 56Cr1 TLS v1.3 KDF KDF SSH KDF SSH KDF SSH KDF SSH KDF SSH KDF SSH KDF SP800-108
Message digest	SHA XOF	Message digest	SHA-1:N/A SHA2-224:N/A SHA2-256:N/A SHA2-384:N/A SHA2-512:N/A SHA2-512/224:N/A SHA2-512/256:N/A SHA3-224:N/A SHA3-256:N/A SHA3-384:N/A SHA3-512:N/A SHAKE-128:N/A SHAKE-256:N/A	SHA-1 SHA-1 SHA-1 SHA-1 SHA-1 SHA-1 SHA-1 SHA2-224 SHA2-224 SHA2-224 SHA2-224 SHA2-224 SHA2-224 SHA2-224 SHA2-224

Name	Type	Description	Properties	Algorithms
				SHA2-256
				SHA2-256
				SHA2-256
				SHA2-256
				SHA2-256
				SHA2-256
				SHA2-256
				SHA2-256
				SHA2-384
				SHA2-384
				SHA2-384
				SHA2-384
				SHA2-384
				SHA2-384
				SHA2-384
				SHA2-512
				SHA2-512
				SHA2-512
				SHA2-512
				SHA2-512
				SHA2-512
				SHA2-512
				SHA2-512/224
				SHA2-512/224
				SHA2-512/224
				SHA2-512/224
				SHA2-512/224
				SHA2-512/224
				SHA2-512/224
				SHA2-512/256
				SHA2-512/256
				SHA2-512/256
				SHA2-512/256
				SHA2-512/256
				SHA2-512/256
				SHA2-512/256
				SHA3-224
				SHA3-224
				SHA3-224
				SHA3-256
				SHA3-256
				SHA3-256
				SHA3-384
				SHA3-384
				SHA3-384
				SHA3-512
				SHA3-512
				SHA3-512
				SHAKE-128
				SHAKE-128
				SHAKE-128
				SHAKE-256

Name	Type	Description	Properties	Algorithms
				SHAKE-256 SHAKE-256
Password-based key derivation	PBKDF	Deriving keys from a password-based KDF	PBKDF:112-256 bits	PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF
Random number generation	DRBG	Random number generation	Counter DRBG:128, 192, 256 bits HMAC DRBG:128, 256 bits Hash DRBG:128, 256 bits	Counter DRBG HMAC DRBG Hash DRBG

Table 8: Security Function Implementations

2.7 Algorithm Specific Information

2.7.1 AES GCM IV

For TLS 1.2, the module offers the AES GCM implementation and uses the context of Scenario 1 of FIPS 140-3 IG C.H. The module is compliant with SP 800-52r2 Section 3.3.1 and the mechanism for IV generation is compliant with RFC 5288 and 8446.

The module does not implement the TLS protocol. The module's implementation of AES GCM is used together with an application that runs outside the module's cryptographic boundary. The design of the TLS 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.

Alternatively, the Crypto Officer can use the module's API to perform AES GCM encryption using internal IV generation. These IVs are always 96 bits and generated using the approved DRBG internal to the module's boundary in compliance with Scenario 2 of IG C.H.

The module also provides a non-approved AES GCM encryption service which accepts arbitrary external IVs from the operator. The service can be requested by invoking the `EVP_EncryptInit_ex2` API function with a non-NULL iv value. When this is the case, the API will set a non-approved service indicator as described in Section 4.3.

Finally, for TLS 1.3, the AES GCM implementation uses the context of Scenario 5 of FIPS 140-3 IG C.H. The protocol that provides this compliance is TLS 1.3, defined in

RFC8446 of August 2018, using the cipher-suites that explicitly select AES GCM as the encryption/decryption cipher (Appendix B.4 of RFC8446). The module supports acceptable AES GCM cipher suites from Section 3.3.1 of SP800-52r2. The module's implementation of AES GCM is used together with an application that runs outside the module's cryptographic boundary. The design of the TLS 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

2.7.2 AES XTS

In accordance to FIPS 140-3 IG C.I, the module implements a check that ensures, before performing any cryptographic operation, that the two AES keys used in AES XTS mode are not identical.

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

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

2.7.3 Key Derivation using SP 800-132 PBKDF2

The module provides password-based key derivation (PBKDF2), compliant with SP 800-132. The module supports option 1a from Section 5.4 of SP 800-132, in which the Master Key (MK) or a segment of it is used directly as the Data Protection Key (DPK). In accordance to SP 800-132 and FIPS 140-3 IG D.N, the following requirements shall be met:

- Derived keys shall only be used in storage applications. The MK shall not be used for other purposes. The module accepts a minimum length of 112 bits for the MK or DPK.
- Passwords or passphrases, used as an input for the PBKDF2, shall not be used as cryptographic keys.
- The minimum length of the password or passphrase accepted by the module is 8 characters. Assuming the worst-case scenario of all digits, this results in the estimated probability of guessing the password to be at most 10^{-8} . Combined with the minimum iteration count as described below, this provides an acceptable trade-off between user experience and security against brute-force attacks.
- A portion of the salt, with a length of at least 128 bits (this is verified by the module to determine the service is approved), shall be generated randomly using the SP 800-90Ar1 DRBG provided by the module.
- The iteration count shall be selected as large as possible, as long as the time required to generate the key using the entered password is acceptable for the users. The module only allows minimum iteration count to be 1000.

2.7.4 Compliance to SP 800-56Arev3 Assurances

The module offers DH and ECDH shared secret computation services compliant to the SP 800-56Arev3 and meeting IG D.F scenario 2 path (1). The key agreement schemes provided by the module are dhEphem and Unified Model, pertaining to the C(2e, 0s) schemes in section 6.1.2. In order to meet the required assurances listed in section 5.6 of SP 800-56Arev3, the module shall be used together with an application that implements the "TLS protocol" and the following steps shall be performed.

1. The entity using the module, must use the module's "Key pair generation" service for generating DH/ECDH ephemeral keys. This meets the assurances required by key pair owner defined in the section 5.6.2.1 of SP 800-56Arev3.
2. As part of the module's shared secret computation (SSC) service, the module internally performs the public key validation on the peer's public key passed in as input to the SSC function. This meets the public key validity assurance required by the sections 5.6.2.2.2 of SP 800-56Arev3.
3. The module does not support static keys therefore the "assurance of peer's possession of private key" is not applicable.

2.7.5 Legacy Algorithms

The module utilizes the following legacy algorithms as defined in SP 800-131Arev2:

- SHA-1 for RSA Signature Verification and ECDSA Signature Verification purposes.
- RSA Signature Verification, under FIPS 186-4, allows verifying signatures with a bit size of 1024, along with the approved modulus sizes of 2048, 3072, and 4096 bits.
- ECDSA Signature Verification, under FIPS 186-4, allows verifying elliptic curve-based signatures with curve P-192, in addition to the approved curves of P-224, P-256, P-384, and P-521.

2.8 RBG and Entropy

Cert Number	Vendor Name
E62	Canonical Ltd.

Table 9: Entropy Certificates

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
Canonical OpenSSL FIPS provider CPU Time Jitter Entropy source (version 2.2.0)	Non-Physical	Ubuntu 22.04 on Supermicro SYS-1019P-WTR with Intel Xeon Gold 6226; Ubuntu 22.04 on Amazon Web Services (AWS) c6g.metal with AWS Graviton2; Ubuntu 22.04 on IBM z15 with IBM z15	64 bits	Full entropy	AES-256-CTR-DRBG (A3814); AES-256-CTR-DRBG (A3970)

Table 10: Entropy Sources

The module employs two Deterministic Random Bit Generator (DRBG) implementations based on SP 800-90Ar1. These DRBGs are used internally by the module (e.g. to generate seeds for asymmetric key pairs and random numbers for security functions).

They can also be accessed using the specified API functions. The following parameters are used:

4. Private DRBG: AES-256 CTR_DRBG with derivation function. This DRBG is used to generate secret random values (e.g. during asymmetric key pair generation). It can be accessed using `RAND_priv_bytes`.
5. Public DRBG: AES-256 CTR_DRBG with derivation function. This DRBG is used to generate general purpose random values that do not need to remain secret (e.g. initialization vectors). It can be accessed using `RAND_bytes`.

The public and private DRBGs are seeded with 384 bits of entropy and 256 bits of entropy are used to reseed each of the private and public DRBGs. The highest SSP security strength generated by the module is 256 bits.

These DRBGs will always employ prediction resistance. More information regarding the configuration and design of these DRBGs can be found in the module's manual pages.

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 obtained from the SP 800-90Ar1 approved DRBG, compliant with Section 4 of SP 800-133r2. This method does not use the value V as described in Additional Comment 2 of FIPS 140-3 IG D.H. 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.
- RSA key pair generation: compliant with SP 800-133r2, Section 5.1, which maps to FIPS 186-4. The method described in Appendix B.3.6 of FIPS 186-4 ("Probable Primes with Conditions Based on Auxiliary Probable Primes") is used.
- ECC (ECDH and ECDSA) key pair generation: compliant with SP 800-133r2, Section 5.1, which maps to FIPS 186-4. The method described in Appendix B.4.2 of FIPS 186-4 ("Testing Candidates") is used.

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

Additionally, the module implements the following key derivation methods:

- KBKDF: compliant with SP 800-108r1. This implementation can be used to derive secret keys from a pre-existing key-derivation-key.

- KDA OneStep, HKDF: compliant with SP 800-56Cr2. These implementations shall only be used to derive secret keys in the context of an SP 800-56Ar3 key agreement scheme.
- ANS X9.42 KDF (CVL), ANS X9.63 KDF (CVL): compliant with SP 800-135r1. These implementations shall only be used to derive secret keys in the context of an ANS X9.42-2001 resp. ANS X9.63- 2001 key agreement scheme.
- SSH KDF (CVL), TLS 1.2 KDF (CVL), TLS 1.3 KDF (CVL): compliant with SP 800-135r1 and RFC 8446. These implementations shall only be used to derive secret keys in the context of the SSH, TLS 1.2, or TLS 1.3 protocols, respectively.
- PBKDF2: compliant with option 1a of SP 800-132. This implementation shall only be used to derive keys for use in storage applications.

2.10 Key Establishment

The module implements SSP agreement and SSP transport methods as listed in the SFI table.

The module provides Diffie-Hellman (DH) and Elliptic Curve Diffie-Hellman (ECDH) shared secret computation compliant with SP800-56Ar3, in accordance with scenario 2 (1) of FIPS 140-3 IG D.F.

According to FIPS 140-3 IG D.B, for shared secret computation, the key sizes of DH provide 112-200 bits of security strength, while the key sizes of ECDH provide 112-256 bits of security strength in Approved mode of operation.

The module also supports the AES KW and AES KWP key wrapping mechanisms compliant with IG D.G and SP 800-38F. These algorithms can be used to wrap SSPs with a security strength of 128, 192, or 256 bits, depending on the wrapping key size.

2.11 Industry Protocols

The module implements the SSH KDF (CVL) for use in the SSH protocol (RFC 4253 and RFC 6668).

GCM with internal IV generation in the approved mode is compliant with versions 1.2 and 1.3 of the TLS protocol (RFC 5288 and 8446) and shall only be used in conjunction with the TLS protocol. Additionally, the module implements the TLS 1.2 and TLS 1.3 key derivation functions for use in the TLS protocol.

For Diffie-Hellman, the module supports the use of the safe primes defined in RFC 3526 (IKE) and RFC 7919 (TLS). Note that the module only implements key pair generation, key pair verification, and shared secret computation. No other part of the IKE or TLS protocols is implemented (with the exception of the TLS 1.2 KDF (CVL) and 1.3 KDF (CVL)):

- IKE (RFC 3526): MODP-2048 (ID = 14), MODP-3072 (ID = 15), MODP-4096 (ID = 16), MODP-6144 (ID = 17), MODP-8192 (ID = 18)

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

For Elliptic Curve Diffie-Hellman, the module supports the NIST-defined P-224, P-256, P-384, and P-521 curves.

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

2.12 Additional Information

Not applicable.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

Physical Port	Logical Interface(s)	Data That Passes
As a software-only module, the module does not have physical ports. Physical Ports are interpreted to be the physical ports of the hardware platform on which it runs.	Data Input	API input parameters
As a software-only module, the module does not have physical ports. Physical Ports are interpreted to be the physical ports of the hardware platform on which it runs.	Data Output	API output parameters
As a software-only module, the module does not have physical ports. Physical Ports are interpreted to be the physical ports of the hardware platform on which it runs.	Control Input	API function calls
As a software-only module, the module does not have physical ports. Physical Ports are interpreted to be the physical ports of the hardware platform on which it runs.	Status Output	API return codes, error queue

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 table above summarizes the logical interfaces.

As a software-only module, the module does not have physical ports. Physical Ports are interpreted to be the physical ports of the hardware platform on which it runs. The module does not implement a control output interface.

3.2 Trusted Channel Specification

Not applicable.

3.3 Control Interface Not Inhibited

Not applicable.

3.4 Additional Information

Not applicable.

4 Roles, Services, and Authentication

4.1 Authentication Methods

N/A for this module.

4.2 Roles

Name	Type	Operator Type	Authentication Methods
Crypto Officer	Role	CO	None

Table 12: Roles

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

4.3 Approved Services

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Message digest	Compute a message digest	UBUNTU_OSSL_PROV_FIPS_PARAM_UNAPPROVED_USAGE returns 0	Message	Message digest	Message digest	Crypto Officer
Symmetric encryption	Encrypt a plaintext	UBUNTU_OSSL_PROV_FIPS_PARAM_UNAPPROVED_USAGE returns 0	AES key, Plaintext	Ciphertext	Symmetric encryption	Crypto Officer - AES key: W,E
Symmetric decryption	Decrypt a ciphertext	UBUNTU_OSSL_PROV_FIPS_PARAM_UNAPPROVED_USAGE returns 0	AES key, Ciphertext	Plaintext	Symmetric decryption	Crypto Officer - AES key: W,E
Authenticated symmetric encryption	Encrypt and authenticate a plaintext	UBUNTU_OSSL_PROV_FIPS_PARAM_UNAPPROVED_USAGE returns 0	AES key, Plaintext, IV	Ciphertext, MAC tag	Symmetric encryption	Crypto Officer - AES key: W,E
Authenticated symmetric decryption	Decrypt and authenticate a ciphertext	UBUNTU_OSSL_PROV_FIPS_PARAM_UNAPPROVED_USAGE returns 0	AES key, Ciphertext, MAC tag	Plaintext or Failure	Symmetric decryption	Crypto Officer - AES key: W,E
Key wrapping	Perform AES-based key wrapping	UBUNTU_OSSL_PROV_FIPS_PARAM_UNAPPROVED_USAGE returns 0	AES key, Key to be wrapped	Wrapped key	Key wrapping	Crypto Officer - AES key: W,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Key unwrapping	Perform AES-based key unwrapping	UBUNTU_OSSL_PROV_FIPS_PARAM_UNAPPROVED_USAGE returns 0	AES key, Key to unwrap	Unwrapped key	Key unwrapping	Crypto Officer - AES key: W,E
AES-based message authentication generation	Compute a MAC tag using AES	UBUNTU_OSSL_PROV_FIPS_PARAM_UNAPPROVED_USAGE returns 0	AES key, Message	MAC tag	Message authentication	Crypto Officer - AES key: W,E
AES-based message authentication verification	Verify a MAC tag using AES	UBUNTU_OSSL_PROV_FIPS_PARAM_UNAPPROVED_USAGE returns 0	AES key, Message, MAC tag	Pass/fail	Message authentication	Crypto Officer - AES key: W,E
HMAC-based message authentication generation	Compute a MAC tag using HMAC	UBUNTU_OSSL_PROV_FIPS_PARAM_UNAPPROVED_USAGE returns 0	HMAC key, Message	MAC tag	Message authentication	Crypto Officer - HMAC key: W,E
HMAC-based message authentication verification	Verify a MAC tag using HMAC	UBUNTU_OSSL_PROV_FIPS_PARAM_UNAPPROVED_USAGE returns 0	HMAC key, Message, MAC tag	Pass/fail	Message authentication	Crypto Officer - HMAC key: W,E
KMAC-based message authentication generation	Compute a MAC tag using KMAC	UBUNTU_OSSL_PROV_FIPS_PARAM_UNAPPROVED_USAGE returns 0	KMAC key, Message	MAC tag	Message authentication	Crypto Officer - KMAC key: W,E
KMAC-based message authentication verification	Verify MAC tag using KMAC	UBUNTU_OSSL_PROV_FIPS_PARAM_UNAPPROVED_USAGE returns 0	KMAC key, Message, MAC tag	Pass/fail	Message authentication	Crypto Officer - KMAC key: W,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
TLS-based key derivation	TLS key derivation	UBUNTU_OSSL_PROV_FIPS_PARAM_UNAPPROVED_USAGE returns 0	Shared secret	TLS Derived key	Key derivation	Crypto Officer - Shared secret: W,E - TLS Derived key: G,R
Key-based key derivation	Derive a key from a key-derivation key	UBUNTU_OSSL_PROV_FIPS_PARAM_UNAPPROVED_USAGE returns 0	Key-derivation key	KBKDF Derived key	Key derivation	Crypto Officer - Key-derivation key: W,E - KBKDF Derived key: G,R
ANS X9.42 key derivation	Derive a key from a shared secret	UBUNTU_OSSL_PROV_FIPS_PARAM_UNAPPROVED_USAGE returns 0	Shared secret	ANS X9.42 Derived key	Key derivation	Crypto Officer - Shared secret: W,E - ANS X9.42 Derived key: G,R
ANS X9.63 key derivation	Derive a key from a shared secret	UBUNTU_OSSL_PROV_FIPS_PARAM_UNAPPROVED_USAGE returns 0	Shared secret	ANS X9.63 Derived key	Key derivation	Crypto Officer - Shared secret: W,E - ANS X9.63 Derived key: G,R
HKDF key derivation	Derive a key from a shared secret	UBUNTU_OSSL_PROV_FIPS_PARAM_UNAPPROVED_USAGE returns 0	Shared secret	HKDF Derived key	Key derivation	Crypto Officer - Shared secret: W,E - HKDF Derived key: G,R
OneStep KDA key derivation	Derive a key from a shared secret	UBUNTU_OSSL_PROV_FIPS_PARAM_UNAPPROVED_USAGE returns 0	Shared secret	OneStep KDA Derived key	Key derivation	Crypto Officer - Shared secret: W,E - OneStep

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						KDA Derived key: G,R
SSH KDF key derivation	Derive a key from a shared secret	UBUNTU_OSSL_PROV_FIPS_PARAM_UNA PPROVED_USAGE returns 0	Shared secret	SSH KDF Derived key	Key derivation	Crypto Officer - Shared secret: W,E - SSH KDF Derived key: G,R
Password-based key derivation	Derive a key from a password	UBUNTU_OSSL_PROV_FIPS_PARAM_UNA PPROVED_USAGE returns 0	Password	PBKDF Derived key	Password-based key derivation	Crypto Officer - Password: W,E,Z - PBKDF Derived key: G,R
Random number generation	Generate random number	UBUNTU_OSSL_PROV_FIPS_PARAM_UNA PPROVED_USAGE returns 0	Number of bits	Random number	Random number generation	Crypto Officer - Entropy input: W,E - DRBG Internal state (V, Key): G,W,E - DRBG Internal state (V, C): G,W,E - DRBG seed: G,W,E
Diffie-Hellman shared secret computation	Compute a shared secret	UBUNTU_OSSL_PROV_FIPS_PARAM_UNA PPROVED_USAGE returns 0	DH private key (owner), DH public key (peer)	Shared secret	Shared secret computation	Crypto Officer - DH private key: W,E - DH public key: W,E - Shared secret: G,R
EC Diffie-Hellman	Compute a	UBUNTU_OSSL_PROV_FIPS_PARAM_UNA PPROVED_USAGE returns 0	EC private	Shared secret	Shared secret	Crypto Officer

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
shared secret computation	shared secret		key (owner), EC public key (peer)		computation	- EC private key: W,E - EC public key: W,E - Shared secret: G,R
RSA Digital signature generation	Generate a digital signature with RSA	UBUNTU_OSSL_PROV_FIPS_PARAM_UNAPPROVED_USAGE returns 0	RSA private key, Message, Hash algorithm	Signature	Digital signature generation	Crypto Officer - RSA private key: W,E
ECDSA digital signature generation	Generate a digital signature with ECDSA	UBUNTU_OSSL_PROV_FIPS_PARAM_UNAPPROVED_USAGE returns 0	EC private key, Message, Hash algorithm	Signature	Digital signature generation	Crypto Officer - EC private key: W,E
RSA Digital signature verification	Verify a digital signature using RSA	UBUNTU_OSSL_PROV_FIPS_PARAM_UNAPPROVED_USAGE returns 0	RSA public key, Message, Signature, Hash algorithm	Pass or Fail	Digital signature verification	Crypto Officer - RSA public key: W,E
ECDSA digital signature verification	Verify a digital signature using RSA	UBUNTU_OSSL_PROV_FIPS_PARAM_UNAPPROVED_USAGE returns 0	EC public key, Message, Signature, Hash algorithm	Pass or Fail	Digital signature verification	Crypto Officer - EC public key: W,E
RSA key pair generation	Generate an RSA key pair	UBUNTU_OSSL_PROV_FIPS_PARAM_UNAPPROVED_USAGE returns 0	Key length	RSA private key, RSA public key	Key pair generation	Crypto Officer - RSA private key: G,R - RSA public

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						key: G,R - Intermediate key generation value: G,E,Z
ECDSA key pair generation	Generate an EC key pair	UBUNTU_OSSL_PROV_FIPS_PARAM_UNAPPROVED_USAGE returns 0	Key length	EC private key, EC public key	Key pair generation	Crypto Officer - EC private key: G,R - EC public key: G,R - Intermediate key generation value: G,E,Z
Safe primes key pair generation	Generate an DH key pair	UBUNTU_OSSL_PROV_FIPS_PARAM_UNAPPROVED_USAGE returns 0	Group	DH private key, DH public key	Key pair generation	Crypto Officer - DH private key: G,R - DH public key: G,R - Intermediate key generation value: G,E,Z
ECDSA key pair verification	Verify an EC key pair	UBUNTU_OSSL_PROV_FIPS_PARAM_UNAPPROVED_USAGE returns 0	EC private key, EC public key	Pass or Fail	Key pair verification	Crypto Officer - EC private key: E,W - EC public key: E,W
Safe prime key pair verification	Verify a DH key pair	UBUNTU_OSSL_PROV_FIPS_PARAM_UNAPPROVED_USAGE returns 0	DH private key, DH public key	Pass or Fail	Key pair verification	Crypto Officer - DH private key: E,W - DH public key: E,W

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Show version	Return the name and version information	UBUNTU_OSSL_PROV_FIPS_PARAM_UNAPPROVED_USAGE returns 0	None	Module name and version	None	Crypto Officer
Show status	Return the module status	UBUNTU_OSSL_PROV_FIPS_PARAM_UNAPPROVED_USAGE returns 0	None	Module status	None	Crypto Officer
Self-test	Perform the CASTs and integrity test	None	None	Pass or Fail of self-tests	None	Crypto Officer
Zeroization	Zeroize any SSP	None	An SSP	None	None	Crypto Officer - AES key: Z - HMAC key: Z - KMAC key: Z - Key-derivation key: Z - Shared secret: Z - Password: Z - PBKDF Derived key: Z - KBKDF Derived key: Z - ANS X9.42 Derived key: Z - ANS X9.63 Derived key: Z - HKDF Derived key: Z -

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						OneStep KDA Derived key: Z - TLS Derived key: Z - Entropy input: Z - DRBG Internal state (V, Key): Z - DRBG Internal state (V, C): Z - DRBG seed: Z - DH private key: Z - DH public key: Z - EC private key: Z - EC public key: Z - RSA private key: Z - RSA public key: Z - Intermed iate key generati on value: Z

Table 13: Approved Services

The module provides services to operators that assume the available role. All services are described in detail in the API documentation (manual pages). The Approved Services table and the Non-Approved Services table define the services that utilize approved and non-approved security functions in this module. For the respective tables, the convention below applies when specifying the access permissions (types) that the service has for each SSP.

- **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.

To interact with the module, a calling application must use the EVP API layer provided by OpenSSL. This layer will delegate the request to the FIPS provider, which will in turn perform the requested service. Additionally, this EVP API layer can be used to retrieve the approved service indicator for the module.

The cryptographic module provides an approved service indicator in the form of an OpenSSL provider gettable parameter called `UBUNTU_OSSL_PROV_FIPS_PARAM_UNAPPROVED_USAGE`. This parameter will be equal to 0 if the requested service is an approved security service, otherwise it will be set to 1. The operator is responsible to query the value of such gettable parameter after calling the requested service.

4.4 Non-Approved Services

Name	Description	Algorithms	Role
Encryption	AES GCM (external IV)	AES GCM (external IV)	CO
DSA	Key pair generation; Key pair verification; Signature generation; Signature verification	DSA	CO
ECDSA with curve P-192	Key pair generation	ECDSA with curve P-192	CO
RSA and ECDSA (pre-hashed message)	Signature generation (pre-hashed message); Signature verification (pre-hashed message)	RSA and ECDSA (pre-hashed message)	CO
RSA X9.31	Signature generation; Signature verification	RSA X9.31	CO
RSA primitive	Asymmetric encryption; Asymmetric decryption	RSA primitive	CO
RSA-OAEP	Asymmetric encryption; Asymmetric decryption	RSA-OAEP	CO
RSASVE	Secret value encapsulation; Secret value decapsulation	RSASVE	CO

Table 14: Non-Approved Services

The table above lists the non-approved services in this module, the algorithms involved, the roles that can request the service. In this table, CO specifies the Crypto Officer role.

4.5 External Software/Firmware Loaded

The module does not have the capability of loading software or firmware from an external source.

4.6 Bypass Actions and Status

Not applicable.

4.7 Cryptographic Output Actions and Status

Not applicable.

4.8 Additional Information

Not applicable.

5 Software/Firmware Security

5.1 Integrity Techniques

The integrity of the module is verified by comparing a HMAC-SHA2-256 value calculated at run time with the HMAC-SHA2-256 value embedded in the fips.so file that was computed at build time.

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 test may be invoked on-demand by unloading and subsequently re-initializing the module, or by calling the `OSSL_PROVIDER_self_test` function. This will perform (among others) the software integrity test.

5.3 Open-Source Parameters

Not applicable.

5.4 Additional Information

Not applicable.

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Modifiable

How Requirements are Satisfied:

The module shall be installed as stated in Section 11. If properly installed, the operating system provides process isolation and memory protection mechanisms that ensure appropriate separation for memory access among the processes on the system. Each process has control over its own data and uncontrolled access to the data of other processes is prevented.

6.2 Configuration Settings and Restrictions

Instrumentation tools like the ptrace system call, gdb and strace, userspace live patching, 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.

6.3 Additional Information

There are no concurrent operators.

7 Physical Security

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

7.1 Mechanisms and Actions Required

N/A for this module.

7.2 User Placed Tamper Seals

Number: Not applicable.

Placement: Not applicable.

Surface Preparation: Not applicable.

Operator Responsible for Securing Unused Seals: Not applicable.

Part Numbers: Not applicable.

7.3 Filler Panels

Not applicable.

7.4 Fault Induction Mitigation

Not applicable.

7.5 EFP/EFT Information

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

Table 15: EFP/EFT Information

Not applicable.

7.6 Hardness Testing Temperature Ranges

Temperature Type	Temperature
LowTemperature	
HighTemperature	

Table 16: Hardness Testing Temperatures

Not applicable.

7.7 Additional Information

Not applicable.

8 Non-Invasive Security

8.1 Mitigation Techniques

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

8.2 Effectiveness

Not applicable.

8.3 Additional Information

Not applicable.

9 Sensitive Security Parameters Management

9.1 Storage Areas

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

Table 17: Storage Areas

SSPs are provided to the module by the calling application and are destroyed when released by the appropriate API function calls. The module does not perform persistent storage of SSPs.

9.2 SSP Input-Output Methods

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

Table 18: SSP Input-Output Methods

The module only supports SSP entry and output to and from the calling application running on the same operational environment. This corresponds to manual distribution, electronic entry/output (“CM Software to/from App via TOEPP Path”) per FIPS 140-3 IG 9.5.A Table 1. There is no entry or output of cryptographically protected SSPs.

SSPs can be entered into the module via API input parameters, when required by a service. SSPs can also be output from the module via API output parameters, immediately after generation of the SSP (see Section 9.2).

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Free cipher handle	Zeroizes the SSPs contained within the cipher handle: <code>EVP_CIPHER_CTX_free()</code> clears and frees symmetric cipher context, <code>EVP_MAC_CTX_free()</code> clears and frees MAC context, <code>EVP_KDF_CTX_free()</code> clears and frees KDF context, <code>EVP_RAND_CTX_free()</code> clears and frees DRBG context, <code>EVP_PKEY_free()</code> clears and frees asymmetric key pair structures	Memory occupied by SSPs is overwritten with zeroes and then it is released, which renders the SSP values irretrievable. The completion of the zeroization routine indicates that the zeroization procedure succeeded	By calling the cipher related zeroization API

Zeroization Method	Description	Rationale	Operator Initiation
Automatic	Automatically zeroized by the module when no longer needed	Memory occupied by SSPs is overwritten with zeroes, which renders the SSP values irretrievable.	N/A
Module reset	De-allocates the volatile memory used to store SSPs	Volatile memory used by the module is overwritten within nanoseconds when power is removed.	By unloading and reloading the module

Table 19: SSP Zeroization Methods

The memory occupied by SSPs is allocated by regular memory allocation operating system calls. The operator is responsible for calling the appropriate destruction functions provided in the module's API. The destruction functions, listed above, overwrite the memory occupied by SSPs with zeroes and de-allocate the memory with the regular memory de-allocation operating system call. All data output is inhibited during zeroization.

9.4 SSPs

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
AES key	Used for encryption, decryption, and message authentication	128, 192, 256 bits - 128, 192, 256 bits	Symmetric key - CSP			Symmetric encryption Symmetric decryption Message authentication
HMAC key	Used for hash-based message authentication	112-524288 bits - 112-256 bits	Symmetric key - CSP			Message authentication
KMAC key	Used for message authentication	128-1024 bits - 128-256 bits	Symmetric key - CSP			Message authentication
Key-derivation key	Used for key derivation	112-4096 bits - 112-256 bits	Symmetric key - CSP			Key derivation
Shared secret	Generated by shared secret computation and used for key derivation	224-8192 bits - 112-256 bits	Shared secret - CSP		Shared secret computation	Key derivation
Password	Used for password-based key derivation	At least 8 characters - N/A	Password - CSP			Password-based key derivation
PBKDF Derived key	Generated from password-	112-256 bits - 112-256 bits	Symmetric key - CSP	Key derivation		Key derivation

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	based key derivation					
KBKDF Derived key	Generated from key-based key derivation	112-256 bits - 112-256 bits	Symmetric key - CSP	Key derivation		Key derivation
ANS X9.42 Derived key	Generated from ANS X9.42 key derivation	112-256 bits - 112-256 bits	Symmetric key - CSP	Key derivation		Key derivation
ANS X9.63 Derived key	Generated from ANS X9.63 key derivation	112-256 bits - 112-256 bits	Symmetric key - CSP	Key derivation		Key derivation
HKDF Derived key	Generated from HKDF key derivation	112-256 bits - 112-256 bits	Symmetric key - CSP	Key derivation		Key derivation
OneStep KDA Derived key	Generated from OneStep KDA key derivation	112-256 bits - 112-256 bits	Symmetric key - CSP	Key derivation		Key derivation
TLS Derived key	Generated by TLS-based key derivation	112-256 bits - 112-256 bits	Symmetric key - CSP	Key derivation		Key derivation
Entropy input	Used for random number generation and seeding a DRBG (compliant with IG D.L)	128-384 bits - 128-256 bits	Entropy Input - CSP			Random number generation
DRBG Internal state (V, Key)	Used for random number generation (compliant with IG D.L)	CTR_DRBG: 256, 320, 348 bits; HMAC_DRBG: 320, 512, 1024 bits - CTR_DRBG: 128, 192, 256 bits; HMAC_DRBG: 128, 256 bits	Internal state - CSP	Random number generation		Random number generation
DRBG Internal state (V, C)	Used for random number generation (compliant with IG D.L)	880, 1776 bits - 128, 256 bits	Internal state - CSP	Random number generation		Random number generation
DRBG seed	Used for random number generation	128-256 bits - 128-256 bits	Seed - CSP	Random number generation		Random number generation

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	(compliant with IG D.L)					
DH private key	Used for shared secret computation and key pair verification	2048-8192 bits - 112-200 bits	Private key - CSP	Key pair generation		Shared secret computation Key pair verification
DH public key	Used for shared secret computation and key pair verification	2048-8192 bits - 112-200 bits	Public key - PSP	Key pair generation		Shared secret computation Key pair verification
EC private key	Used for shared secret computation, digital signature generation, and key pair verification	P-224, P-256, P-384, P-521, K-233, K-283, K-409, K-571, B-233, B-283, B-409, B-571 bits - 112, 128, 192, 256 bits	Private key - CSP	Key pair generation		Digital signature generation Shared secret computation Key pair verification
EC public key	Used for shared secret computation, signature verification, and key pair verification	P-192, P-224, P-256, P-384, P-521, K-163, K-233, K-283, K-409, K-571, B-163, B-233, B-283, B-409, B-571 bits - 96, 112, 128, 192, 256 bits	Public key - PSP	Key pair generation		Digital signature verification Shared secret computation Key pair verification
RSA private key	Used for signature generation	2048-16384 bits - 112-256 bits	Private key - CSP	Key pair generation		Digital signature generation
RSA public key	Used for signature verification	1024-16384 bits - 80-256 bits	Public key - PSP	Key pair generation		Digital signature verification
Intermediate key generation value	Used for key pair generation	112-16384 bits - 112-256 bits	intermediate key generation value - CSP	Key pair generation		Key pair generation
SSH KDF Derived key	Generated from SSH KDF key derivation	112-256 bits - 112-256 bits	Symmetric key - CSP	Key derivation		

Table 20: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
AES key	API input parameters	RAM:Plaintext	From service invocation to service completion	Free cipher handle Module reset	
HMAC key	API input parameters	RAM:Plaintext	From service invocation to service completion	Free cipher handle Module reset	
KMAC key	API input parameters	RAM:Plaintext	From service invocation to service completion	Free cipher handle Module reset	
Key-derivation key	API input parameters	RAM:Plaintext	From service invocation to service completion	Free cipher handle Module reset	KBKDF Derived key:Derives
Shared secret	API input parameters API output parameters	RAM:Plaintext	From service invocation to service completion	Free cipher handle Module reset	DH private key:Generated From DH public key:Generated From EC private key:Generated From EC public key:Generated From OneStep KDA Derived key:Derives HKDF Derived key:Derives ANS X9.42 Derived key:Derives ANS X9.63 Derived key:Derives TLS Derived key:Derives SSH KDF Derived key:Derives
Password	API input parameters	RAM:Plaintext	From service invocation to service completion	Free cipher handle Module reset	PKBDF Derived key:Derives
PBKDF Derived key	API output parameters	RAM:Plaintext	From service invocation to service completion	Free cipher handle Module reset	Password:Derived From
KBKDF Derived key	API output parameters	RAM:Plaintext	From service invocation to service completion	Free cipher handle Module reset	Key derivation key:Derived From

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
ANS X9.42 Derived key	API output parameters	RAM:Plaintext	From service invocation to service completion	Free cipher handle Module reset	Shared secret:Derived From
ANS X9.63 Derived key	API output parameters	RAM:Plaintext	From service invocation to service completion	Free cipher handle Module reset	Shared secret:Derived From
HKDF Derived key	API output parameters	RAM:Plaintext	From service invocation to service completion	Free cipher handle Module reset	Shared secret:Derived From
OneStep KDA Derived key	API output parameters	RAM:Plaintext	From service invocation to service completion	Free cipher handle Module reset	Shared secret:Derived From
TLS Derived key	API output parameters	RAM:Plaintext	From service invocation to service completion	Free cipher handle Module reset	Shared secret:Derived From
Entropy input		RAM:Plaintext	From service invocation to service completion	Automatic Module reset	DRBG seed:Generates
DRBG Internal state (V, Key)		RAM:Plaintext	From DRBG instantiation to un-instantiation or internal zeroization	Free cipher handle Module reset	DRBG seed:Generated From
DRBG Internal state (V, C)		RAM:Plaintext	From DRBG instantiation to un-instantiation or internal zeroization	Free cipher handle Module reset	DRBG seed:Generated From
DRBG seed		RAM:Plaintext	From service invocation to service completion	Automatic Module reset	DRBG Internal state (V, Key):Generates DRBG Internal state (V, C):Generates
DH private key	API input parameters API output parameters	RAM:Plaintext	From service invocation to service completion	Free cipher handle Module reset	DH public key:Paired With Intermediate key generation value:Generated From Shared secret:Generates
DH public key	API input parameters API output parameters	RAM:Plaintext	From service invocation to service completion	Free cipher handle Module reset	DH private key:Paired With Intermediate key generation value:Generated From Shared secret:Generates

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
EC private key	API input parameters API output parameters	RAM:Plaintext	From service invocation to service completion	Free cipher handle Module reset	EC public key:Paired With Intermediate key generation value:Generated By Shared secret:Generates
EC public key	API input parameters API output parameters	RAM:Plaintext	From service invocation to service completion	Free cipher handle Module reset	EC private key:Paired With Intermediate key generation value:Generated By Shared secret:Generates
RSA private key	API input parameters API output parameters	RAM:Plaintext	From service invocation to service completion	Free cipher handle Module reset	RSA public key:Paired With Intermediate key generation value:Generated By
RSA public key	API input parameters API output parameters	RAM:Plaintext	From service invocation to service completion	Free cipher handle Module reset	RSA private key:Paired With Intermediate key generation value:Generated From
Intermediate key generation value		RAM:Plaintext	From service invocation to service completion	Automatic	RSA private key:Generates EC private key:Generates DH private key:Generates RSA public key:Generates EC public key:Generates DH public key:Generates
SSH KDF Derived key	API output parameters	RAM:Plaintext	From service invocation to service completion	Free cipher handle Module reset	Shared secret:Derived From

Table 21: SSP Table 2

The tables above summarize the Sensitive Security Parameters (SSPs) that are used by the cryptographic services implemented in the module in the approved services (Approved Services table).

SSPs, including CSPs, are directly imported as input parameters and exported as output parameters from the module. Because these SSPs are only transiently used for a specific service, they are, by definition, exclusive between approved and non-approved services.

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 has been withdrawn since February 3, 2024.

9.6 Additional Information

Not applicable.

10 Self-Tests

10.1 Pre-Operational Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
HMAC-SHA2-256 (A3962)	256-bit key	Message Authentication	SW/FW Integrity	Module becomes operational and services are available for use	Integrity test for fips.so
HMAC-SHA2-256 (A3963)	256-bit key	Message Authentication	SW/FW Integrity	Module becomes operational and services are available for use	Integrity test for fips.so
HMAC-SHA2-256 (A3977)	256-bit key	Message Authentication	SW/FW Integrity	Module becomes operational and services are available for use	Integrity test for fips.so
HMAC-SHA2-256 (A3983)	256-bit key	Message Authentication	SW/FW Integrity	Module becomes operational and services are available for use	Integrity test for fips.so
HMAC-SHA2-256 (A3993)	256-bit key	Message Authentication	SW/FW Integrity	Module becomes operational and services are available for use	Integrity test for fips.so
HMAC-SHA2-256 (A4003)	256-bit key	Message Authentication	SW/FW Integrity	Module becomes operational and services are available for use	Integrity test for fips.so
HMAC-SHA2-256 (A4004)	256-bit key	Message Authentication	SW/FW Integrity	Module becomes operational and services are available for use	Integrity test for fips.so
HMAC-SHA2-256 (A4005)	256-bit key	Message Authentication	SW/FW Integrity	Module becomes operational and services are available for use	Integrity test for fips.so

Table 22: Pre-Operational Self-Tests

The module performs pre-operational tests automatically when the module is powered on. The pre-operational self-tests ensure that the module is not corrupted. The module transitions to the operational state only after the pre-operational self-tests are passed successfully.

The integrity of the shared library component of the module is verified by comparing an HMAC-SHA2-256 value calculated at run time with the corresponding HMAC value embedded in the fips.so file that was computed at build time.

If the software integrity test fails, the module transitions to the error state (Section 10.3). The HMAC and SHA2-256 algorithms go through their respective CASTs before the software integrity test is performed.

10.2 Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
SHA-1 (A3962)	24-bit message	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA-1 (A3977)	24-bit message	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA-1 (A3983)	24-bit message	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA-1 (A3993)	24-bit message	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA-1 (A4003)	24-bit message	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA-1 (A4004)	24-bit message	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA-1 (A4005)	24-bit message	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-512 (A3962)	24-bit message	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-512 (A3977)	24-bit message	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-512 (A3983)	24-bit message	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-512 (A3993)	24-bit message	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
SHA2-512 (A4003)	24-bit message	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-512 (A4004)	24-bit message	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-512 (A4005)	24-bit message	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA3-256 (A3964)	32-bit message	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA3-256 (A3972)	32-bit message	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA3-256 (A3979)	32-bit message	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
AES-GCM (A3961)	Encrypt with 256-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3974)	Encrypt with 256-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3975)	Encrypt with 256-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3976)	Encrypt with 256-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3988)	Encrypt with 256-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3989)	Encrypt with 256-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-GCM (A3990)	Encrypt with 256-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3994)	Encrypt with 256-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3995)	Encrypt with 256-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3996)	Encrypt with 256-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3997)	Encrypt with 256-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3998)	Encrypt with 256-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3999)	Encrypt with 256-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A4000)	Encrypt with 256-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A4001)	Encrypt with 256-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A4002)	Encrypt with 256-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3961)	Decrypt with 256-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3974)	Decrypt with 256-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-GCM (A3975)	Decrypt with 256-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3976)	Decrypt with 256-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3988)	Decrypt with 256-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3989)	Decrypt with 256-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3990)	Decrypt with 256-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3994)	Decrypt with 256-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3995)	Decrypt with 256-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3996)	Decrypt with 256-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3997)	Decrypt with 256-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3998)	Decrypt with 256-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A3999)	Decrypt with 256-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A4000)	Decrypt with 256-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-GCM (A4001)	Decrypt with 256-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A4002)	Decrypt with 256-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3958)	Decrypt with 256-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3959)	Decrypt with 256-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3960)	Decrypt with 256-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3971)	Decrypt with 256-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3973)	Decrypt with 256-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3978)	Decrypt with 256-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3980)	Decrypt with 256-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3981)	Decrypt with 256-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3982)	Decrypt with 256-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3984)	Decrypt with 256-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-ECB (A3985)	Decrypt with 256-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3986)	Decrypt with 256-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A3987)	Decrypt with 256-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
KDF SP800-108 (A3991)	HMAC-SHA2-256 in counter mode	KAT	CAST	Module becomes operational	Key based key derivation	Test runs at power-on before the integrity test
KDA OneStep SP800-56Cr2 (A3965)	SHA2-224	KAT	CAST	Module becomes operational	Shared secret key derivation	Test runs at power-on before the integrity test
KDA HKDF Sp800-56Cr1 (A3969)	SHA2-256	KAT	CAST	Module becomes operational	Shared secret key derivation	Test runs at power-on before the integrity test
KDF ANS 9.42 (A3962)	SHA-1	KAT	CAST	Module becomes operational	Industry-based ANS X9.42 key derivation	Test runs at power-on before the integrity test
KDF ANS 9.42 (A3964)	SHA-1	KAT	CAST	Module becomes operational	Industry-based ANS X9.42 key derivation	Test runs at power-on before the integrity test
KDF ANS 9.42 (A3972)	SHA-1	KAT	CAST	Module becomes operational	Industry-based ANS X9.42 key derivation	Test runs at power-on before the integrity test
KDF ANS 9.42 (A3977)	SHA-1	KAT	CAST	Module becomes operational	Industry-based ANS X9.42 key derivation	Test runs at power-on before the integrity test
KDF ANS 9.42 (A3979)	SHA-1	KAT	CAST	Module becomes operational	Industry-based ANS X9.42 key derivation	Test runs at power-on before the integrity test
KDF ANS 9.42 (A3983)	SHA-1	KAT	CAST	Module becomes operational	Industry-based ANS X9.42 key derivation	Test runs at power-on before the integrity test

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
KDF ANS 9.42 (A3993)	SHA-1	KAT	CAST	Module becomes operational	Industry-based ANS X9.42 key derivation	Test runs at power-on before the integrity test
KDF ANS 9.42 (A4003)	SHA-1	KAT	CAST	Module becomes operational	Industry-based ANS X9.42 key derivation	Test runs at power-on before the integrity test
KDF ANS 9.42 (A4004)	SHA-1	KAT	CAST	Module becomes operational	Industry-based ANS X9.42 key derivation	Test runs at power-on before the integrity test
KDF ANS 9.42 (A4005)	SHA-1	KAT	CAST	Module becomes operational	Industry-based ANS X9.42 key derivation	Test runs at power-on before the integrity test
KDF ANS 9.63 (A3962)	SHA2-256	KAT	CAST	Module becomes operational	Industry-based ANS X9.63 key derivation	Test runs at power-on before the integrity test
KDF ANS 9.63 (A3977)	SHA2-256	KAT	CAST	Module becomes operational	Industry-based ANS X9.63 key derivation	Test runs at power-on before the integrity test
KDF ANS 9.63 (A3983)	SHA2-256	KAT	CAST	Module becomes operational	Industry-based ANS X9.63 key derivation	Test runs at power-on before the integrity test
KDF ANS 9.63 (A3993)	SHA2-256	KAT	CAST	Module becomes operational	Industry-based ANS X9.63 key derivation	Test runs at power-on before the integrity test
KDF ANS 9.63 (A4003)	SHA2-256	KAT	CAST	Module becomes operational	Industry-based ANS X9.63 key derivation	Test runs at power-on before the integrity test
KDF ANS 9.63 (A4004)	SHA2-256	KAT	CAST	Module becomes operational	Industry-based ANS X9.63 key derivation	Test runs at power-on before the integrity test
KDF ANS 9.63 (A4005)	SHA2-256	KAT	CAST	Module becomes operational	Industry-based ANS X9.63 key derivation	Test runs at power-on before the integrity test
KDF SSH (A3971)	SHA-1	KAT	CAST	Module becomes operational	Industry-based SSH KDF key derivation	Test runs at power-on before the integrity test

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
KDF SSH (A3978)	SHA-1	KAT	CAST	Module becomes operational	Industry-based SSH KDF key derivation	Test runs at power-on before the integrity test
KDF SSH (A3984)	SHA-1	KAT	CAST	Module becomes operational	Industry-based SSH KDF key derivation	Test runs at power-on before the integrity test
KDF SSH (A3985)	SHA-1	KAT	CAST	Module becomes operational	Industry-based SSH KDF key derivation	Test runs at power-on before the integrity test
KDF SSH (A3986)	SHA-1	KAT	CAST	Module becomes operational	Industry-based SSH KDF key derivation	Test runs at power-on before the integrity test
KDF SSH (A3987)	SHA-1	KAT	CAST	Module becomes operational	Industry-based SSH KDF key derivation	Test runs at power-on before the integrity test
TLS v1.2 KDF RFC7627 (A3962)	SHA2-256	KAT	CAST	Module becomes operational	Industry-based TLS v1.2 KDF key derivation	Test runs at power-on before the integrity test
TLS v1.2 KDF RFC7627 (A3977)	SHA2-256	KAT	CAST	Module becomes operational	Industry-based TLS v1.2 KDF key derivation	Test runs at power-on before the integrity test
TLS v1.2 KDF RFC7627 (A3983)	SHA2-256	KAT	CAST	Module becomes operational	Industry-based TLS v1.2 KDF key derivation	Test runs at power-on before the integrity test
TLS v1.2 KDF RFC7627 (A3993)	SHA2-256	KAT	CAST	Module becomes operational	Industry-based TLS v1.2 KDF key derivation	Test runs at power-on before the integrity test
TLS v1.2 KDF RFC7627 (A4003)	SHA2-256	KAT	CAST	Module becomes operational	Industry-based TLS v1.2 KDF key derivation	Test runs at power-on before the integrity test
TLS v1.2 KDF RFC7627 (A4004)	SHA2-256	KAT	CAST	Module becomes operational	Industry-based TLS v1.2 KDF key derivation	Test runs at power-on before the integrity test
TLS v1.2 KDF RFC7627 (A4005)	SHA2-256	KAT	CAST	Module becomes operational	Industry-based TLS v1.2 KDF key derivation	Test runs at power-on before the integrity test

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
TLS v1.3 KDF (A3969)	SHA2-256	KAT	CAST	Module becomes operational	Industry-based TLS v1.3 KDF key derivation	Test runs at power-on before the integrity test
PBKDF (A3962)	SHA2-256 with 4096 iterations and 288-bit salt	KAT	CAST	Module becomes operational	Password-based key derivation	Test runs at power-on before the integrity test
PBKDF (A3964)	SHA2-256 with 4096 iterations and 288-bit salt	KAT	CAST	Module becomes operational	Password-based key derivation	Test runs at power-on before the integrity test
PBKDF (A3972)	SHA2-256 with 4096 iterations and 288-bit salt	KAT	CAST	Module becomes operational	Password-based key derivation	Test runs at power-on before the integrity test
PBKDF (A3977)	SHA2-256 with 4096 iterations and 288-bit salt	KAT	CAST	Module becomes operational	Password-based key derivation	Test runs at power-on before the integrity test
PBKDF (A3979)	SHA2-256 with 4096 iterations and 288-bit salt	KAT	CAST	Module becomes operational	Password-based key derivation	Test runs at power-on before the integrity test
PBKDF (A3983)	SHA2-256 with 4096 iterations and 288-bit salt	KAT	CAST	Module becomes operational	Password-based key derivation	Test runs at power-on before the integrity test
PBKDF (A3993)	SHA2-256 with 4096 iterations and 288-bit salt	KAT	CAST	Module becomes operational	Password-based key derivation	Test runs at power-on before the integrity test
PBKDF (A4003)	SHA2-256 with 4096 iterations and 288-bit salt	KAT	CAST	Module becomes operational	Password-based key derivation	Test runs at power-on before the integrity test
PBKDF (A4004)	SHA2-256 with 4096 iterations and 288-bit salt	KAT	CAST	Module becomes operational	Password-based key derivation	Test runs at power-on before the integrity test
PBKDF (A4005)	SHA2-256 with 4096 iterations and 288-bit salt	KAT	CAST	Module becomes operational	Password-based key derivation	Test runs at power-on before the integrity test
Counter DRBG (A3970)	AES-128 with derivation function and prediction resistance	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HMAC DRBG (A3970)	HMAC-SHA-1 with prediction resistance	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
KAS-FFC-SSC Sp800-56Ar3 (A3992)	ffdhe2048	KAT	CAST	Module becomes operational	Shared secret computation	Test runs at power-on before the integrity test
KAS-ECC-SSC Sp800-56Ar3 (A3962)	P-256	KAT	CAST	Module becomes operational	Shared secret computation	Test runs at power-on before the integrity test
KAS-ECC-SSC Sp800-56Ar3 (A3968)	P-256	KAT	CAST	Module becomes operational	Shared secret computation	Test runs at power-on before the integrity test
KAS-ECC-SSC Sp800-56Ar3 (A3977)	P-256	KAT	CAST	Module becomes operational	Shared secret computation	Test runs at power-on before the integrity test
KAS-ECC-SSC Sp800-56Ar3 (A3983)	P-256	KAT	CAST	Module becomes operational	Shared secret computation	Test runs at power-on before the integrity test
KAS-ECC-SSC Sp800-56Ar3 (A3993)	P-256	KAT	CAST	Module becomes operational	Shared secret computation	Test runs at power-on before the integrity test
KAS-ECC-SSC Sp800-56Ar3 (A4003)	P-256	KAT	CAST	Module becomes operational	Shared secret computation	Test runs at power-on before the integrity test
KAS-ECC-SSC Sp800-56Ar3 (A4004)	P-256	KAT	CAST	Module becomes operational	Shared secret computation	Test runs at power-on before the integrity test
KAS-ECC-SSC Sp800-56Ar3 (A4005)	P-256	KAT	CAST	Module becomes operational	Shared secret computation	Test runs at power-on before the integrity test
HMAC-SHA3-512 (A3964)	SHA3-512	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA3-512 (A3972)	SHA3-512	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HMAC-SHA3-512 (A3979)	SHA3-512	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
RSA SigGen (FIPS186-4) (A3962)	PKCS#1 v1.5 with SHA2-256 and 2048-bit key	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test
RSA SigGen (FIPS186-4) (A3977)	PKCS#1 v1.5 with SHA2-256 and 2048-bit key	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test
RSA SigGen (FIPS186-4) (A3983)	PKCS#1 v1.5 with SHA2-256 and 2048-bit key	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test
RSA SigGen (FIPS186-4) (A3993)	PKCS#1 v1.5 with SHA2-256 and 2048-bit key	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test
RSA SigGen (FIPS186-4) (A4003)	PKCS#1 v1.5 with SHA2-256 and 2048-bit key	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test
RSA SigGen (FIPS186-4) (A4004)	PKCS#1 v1.5 with SHA2-256 and 2048-bit key	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test
RSA SigGen (FIPS186-4) (A4005)	PKCS#1 v1.5 with SHA2-256 and 2048-bit key	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test
RSA SigVer (FIPS186-4) (A3962)	PKCS#1 v1.5 with SHA2-256 and 2048-bit key	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
RSA SigVer (FIPS186-4) (A3977)	PKCS#1 v1.5 with SHA2-256 and 2048-bit key	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
RSA SigVer (FIPS186-4) (A3983)	PKCS#1 v1.5 with SHA2-256 and 2048-bit key	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
RSA SigVer (FIPS186-4) (A3993)	PKCS#1 v1.5 with SHA2-256 and 2048-bit key	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
RSA SigVer (FIPS186-4) (A4003)	PKCS#1 v1.5 with SHA2-256 and 2048-bit key	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
RSA SigVer (FIPS186-4) (A4004)	PKCS#1 v1.5 with SHA2-256 and 2048-bit key	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
RSA SigVer (FIPS186-4) (A4005)	PKCS#1 v1.5 with SHA2-256 and 2048-bit key	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
ECDSA SigGen (FIPS186-4) (A3962)	Curves P-224, B-233 with SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test
ECDSA SigGen (FIPS186-4) (A3964)	Curves P-224, B-233 with SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test
ECDSA SigGen (FIPS186-4) (A3966)	Curves P-224, B-233 with SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test
ECDSA SigGen (FIPS186-4) (A3967)	Curves P-224, B-233 with SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test
ECDSA SigGen (FIPS186-4) (A3972)	Curves P-224, B-233 with SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test
ECDSA SigGen (FIPS186-4) (A3977)	Curves P-224, B-233 with SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test
ECDSA SigGen (FIPS186-4) (A3979)	Curves P-224, B-233 with SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test
ECDSA SigGen (FIPS186-4) (A3983)	Curves P-224, B-233 with SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test
ECDSA SigGen (FIPS186-4) (A3993)	Curves P-224, B-233 with SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
ECDSA SigGen (FIPS186-4) (A4003)	Curves P-224, B-233 with SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test
ECDSA SigGen (FIPS186-4) (A4004)	Curves P-224, B-233 with SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test
ECDSA SigGen (FIPS186-4) (A4005)	Curves P-224, B-233 with SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test
ECDSA SigVer (FIPS186-4) (A3962)	Curves P-224, B-233 with SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
ECDSA SigVer (FIPS186-4) (A3964)	Curves P-224, B-233 with SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
ECDSA SigVer (FIPS186-4) (A3966)	Curves P-224, B-233 with SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
ECDSA SigVer (FIPS186-4) (A3967)	Curves P-224, B-233 with SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
ECDSA SigVer (FIPS186-4) (A3972)	Curves P-224, B-233 with SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
ECDSA SigVer (FIPS186-4) (A3977)	Curves P-224, B-233 with SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
ECDSA SigVer (FIPS186-4) (A3979)	Curves P-224, B-233 with SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
ECDSA SigVer (FIPS186-4) (A3983)	Curves P-224, B-233 with SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
ECDSA SigVer (FIPS186-4) (A3993)	Curves P-224, B-233 with SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
ECDSA SigVer (FIPS186-4) (A4003)	Curves P-224, B-233 with SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
ECDSA SigVer (FIPS186-4) (A4004)	Curves P-224, B-233 with SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
ECDSA SigVer (FIPS186-4) (A4005)	Curves P-224, B-233 with SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
Safe Primes Key Generation (A3992)	SHA-1 password length 24 characters, master key length of 200 bits, iteration count of 4096, and salt length of 288 bits	PCT	PCT	Successful key pair generation	Public key re-computation and comparison with the existing public key per SP800-56Arev3, section 5.6.2.1.4	Key pair generation
RSA KeyGen (FIPS186-4) (A3962)	PKCS#1 v1.5 with SHA2-256	PCT	PCT	Successful key pair generation	Generation of an RSA key pair	Key pair generation
RSA KeyGen (FIPS186-4) (A3977)	PKCS#1 v1.5 with SHA2-256	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
RSA KeyGen (FIPS186-4) (A3983)	PKCS#1 v1.5 with SHA2-256	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
RSA KeyGen (FIPS186-4) (A3993)	PKCS#1 v1.5 with SHA2-256	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
RSA KeyGen (FIPS186-4) (A4003)	PKCS#1 v1.5 with SHA2-256	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
RSA KeyGen (FIPS186-4) (A4004)	PKCS#1 v1.5 with SHA2-256	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
RSA KeyGen (FIPS186-4) (A4005)	PKCS#1 v1.5 with SHA2-256	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
ECDSA KeyGen (FIPS186-4) (A3962)	SHA2-256	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
ECDSA KeyGen (FIPS186-4) (A3966)	SHA2-256	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
ECDSA KeyGen (FIPS186-4) (A3977)	SHA2-256	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
ECDSA KeyGen (FIPS186-4) (A3983)	SHA2-256	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
ECDSA KeyGen (FIPS186-4) (A3993)	SHA2-256	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
ECDSA KeyGen (FIPS186-4) (A4003)	SHA2-256	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
ECDSA KeyGen (FIPS186-4) (A4004)	SHA2-256	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
ECDSA KeyGen (FIPS186-4) (A4005)	SHA2-256	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation

Table 23: Conditional Self-Tests

The module performs self-tests on all approved cryptographic algorithms as part of the approved services supported in the approved mode of operation, using the tests shown in the table above. The CASTs can be performed on demand by unloading and re-initializing the module. Data output through the data output interface is inhibited during the self-tests. If any of these tests fails, the module transitions to the error state.

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
HMAC-SHA2-256 (A3962)	Message Authentication	SW/FW Integrity	On demand	Manually
HMAC-SHA2-256 (A3963)	Message Authentication	SW/FW Integrity	On demand	Manually
HMAC-SHA2-256 (A3977)	Message Authentication	SW/FW Integrity	On demand	Manually
HMAC-SHA2-256 (A3983)	Message Authentication	SW/FW Integrity	On demand	Manually
HMAC-SHA2-256 (A3993)	Message Authentication	SW/FW Integrity	On demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
HMAC-SHA2-256 (A4003)	Message Authentication	SW/FW Integrity	On demand	Manually
HMAC-SHA2-256 (A4004)	Message Authentication	SW/FW Integrity	On demand	Manually
HMAC-SHA2-256 (A4005)	Message Authentication	SW/FW Integrity	On demand	Manually

Table 24: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
SHA-1 (A3962)	KAT	CAST	On Demand	Manually
SHA-1 (A3977)	KAT	CAST	On Demand	Manually
SHA-1 (A3983)	KAT	CAST	On Demand	Manually
SHA-1 (A3993)	KAT	CAST	On Demand	Manually
SHA-1 (A4003)	KAT	CAST	On Demand	Manually
SHA-1 (A4004)	KAT	CAST	On Demand	Manually
SHA-1 (A4005)	KAT	CAST	On Demand	Manually
SHA2-512 (A3962)	KAT	CAST	On Demand	Manually
SHA2-512 (A3977)	KAT	CAST	On Demand	Manually
SHA2-512 (A3983)	KAT	CAST	On Demand	Manually
SHA2-512 (A3993)	KAT	CAST	On Demand	Manually
SHA2-512 (A4003)	KAT	CAST	On Demand	Manually
SHA2-512 (A4004)	KAT	CAST	On Demand	Manually
SHA2-512 (A4005)	KAT	CAST	On Demand	Manually
SHA3-256 (A3964)	KAT	CAST	On Demand	Manually
SHA3-256 (A3972)	KAT	CAST	On Demand	Manually
SHA3-256 (A3979)	KAT	CAST	On Demand	Manually
AES-GCM (A3961)	KAT	CAST	On Demand	Manually
AES-GCM (A3974)	KAT	CAST	On Demand	Manually
AES-GCM (A3975)	KAT	CAST	On Demand	Manually
AES-GCM (A3976)	KAT	CAST	On Demand	Manually
AES-GCM (A3988)	KAT	CAST	On Demand	Manually
AES-GCM (A3989)	KAT	CAST	On Demand	Manually
AES-GCM (A3990)	KAT	CAST	On Demand	Manually
AES-GCM (A3994)	KAT	CAST	On Demand	Manually
AES-GCM (A3995)	KAT	CAST	On Demand	Manually
AES-GCM (A3996)	KAT	CAST	On Demand	Manually
AES-GCM (A3997)	KAT	CAST	On Demand	Manually
AES-GCM (A3998)	KAT	CAST	On Demand	Manually
AES-GCM (A3999)	KAT	CAST	On Demand	Manually
AES-GCM (A4000)	KAT	CAST	On Demand	Manually
AES-GCM (A4001)	KAT	CAST	On Demand	Manually
AES-GCM (A4002)	KAT	CAST	On Demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-GCM (A3961)	KAT	CAST	On Demand	Manually
AES-GCM (A3974)	KAT	CAST	On Demand	Manually
AES-GCM (A3975)	KAT	CAST	On Demand	Manually
AES-GCM (A3976)	KAT	CAST	On Demand	Manually
AES-GCM (A3988)	KAT	CAST	On Demand	Manually
AES-GCM (A3989)	KAT	CAST	On Demand	Manually
AES-GCM (A3990)	KAT	CAST	On Demand	Manually
AES-GCM (A3994)	KAT	CAST	On Demand	Manually
AES-GCM (A3995)	KAT	CAST	On Demand	Manually
AES-GCM (A3996)	KAT	CAST	On Demand	Manually
AES-GCM (A3997)	KAT	CAST	On Demand	Manually
AES-GCM (A3998)	KAT	CAST	On Demand	Manually
AES-GCM (A3999)	KAT	CAST	On Demand	Manually
AES-GCM (A4000)	KAT	CAST	On Demand	Manually
AES-GCM (A4001)	KAT	CAST	On Demand	Manually
AES-GCM (A4002)	KAT	CAST	On Demand	Manually
AES-ECB (A3958)	KAT	CAST	On Demand	Manually
AES-ECB (A3959)	KAT	CAST	On Demand	Manually
AES-ECB (A3960)	KAT	CAST	On Demand	Manually
AES-ECB (A3971)	KAT	CAST	On Demand	Manually
AES-ECB (A3973)	KAT	CAST	On Demand	Manually
AES-ECB (A3978)	KAT	CAST	On Demand	Manually
AES-ECB (A3980)	KAT	CAST	On Demand	Manually
AES-ECB (A3981)	KAT	CAST	On Demand	Manually
AES-ECB (A3982)	KAT	CAST	On Demand	Manually
AES-ECB (A3984)	KAT	CAST	On Demand	Manually
AES-ECB (A3985)	KAT	CAST	On Demand	Manually
AES-ECB (A3986)	KAT	CAST	On Demand	Manually
AES-ECB (A3987)	KAT	CAST	On Demand	Manually
KDF SP800-108 (A3991)	KAT	CAST	On Demand	Manually
KDA OneStep SP800-56Cr2 (A3965)	KAT	CAST	On Demand	Manually
KDA HKDF Sp800-56Cr1 (A3969)	KAT	CAST	On Demand	Manually
KDF ANS 9.42 (A3962)	KAT	CAST	On Demand	Manually
KDF ANS 9.42 (A3964)	KAT	CAST	On Demand	Manually
KDF ANS 9.42 (A3972)	KAT	CAST	On Demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
KDF ANS 9.42 (A3977)	KAT	CAST	On Demand	Manually
KDF ANS 9.42 (A3979)	KAT	CAST	On Demand	Manually
KDF ANS 9.42 (A3983)	KAT	CAST	On Demand	Manually
KDF ANS 9.42 (A3993)	KAT	CAST	On Demand	Manually
KDF ANS 9.42 (A4003)	KAT	CAST	On Demand	Manually
KDF ANS 9.42 (A4004)	KAT	CAST	On Demand	Manually
KDF ANS 9.42 (A4005)	KAT	CAST	On Demand	Manually
KDF ANS 9.63 (A3962)	KAT	CAST	On Demand	Manually
KDF ANS 9.63 (A3977)	KAT	CAST	On Demand	Manually
KDF ANS 9.63 (A3983)	KAT	CAST	On Demand	Manually
KDF ANS 9.63 (A3993)	KAT	CAST	On Demand	Manually
KDF ANS 9.63 (A4003)	KAT	CAST	On Demand	Manually
KDF ANS 9.63 (A4004)	KAT	CAST	On Demand	Manually
KDF ANS 9.63 (A4005)	KAT	CAST	On Demand	Manually
KDF SSH (A3971)	KAT	CAST	On Demand	Manually
KDF SSH (A3978)	KAT	CAST	On Demand	Manually
KDF SSH (A3984)	KAT	CAST	On Demand	Manually
KDF SSH (A3985)	KAT	CAST	On Demand	Manually
KDF SSH (A3986)	KAT	CAST	On Demand	Manually
KDF SSH (A3987)	KAT	CAST	On Demand	Manually
TLS v1.2 KDF RFC7627 (A3962)	KAT	CAST	On Demand	Manually
TLS v1.2 KDF RFC7627 (A3977)	KAT	CAST	On Demand	Manually
TLS v1.2 KDF RFC7627 (A3983)	KAT	CAST	On Demand	Manually
TLS v1.2 KDF RFC7627 (A3993)	KAT	CAST	On Demand	Manually
TLS v1.2 KDF RFC7627 (A4003)	KAT	CAST	On Demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
TLS v1.2 KDF RFC7627 (A4004)	KAT	CAST	On Demand	Manually
TLS v1.2 KDF RFC7627 (A4005)	KAT	CAST	On Demand	Manually
TLS v1.3 KDF (A3969)	KAT	CAST	On Demand	Manually
PBKDF (A3962)	KAT	CAST	On Demand	Manually
PBKDF (A3964)	KAT	CAST	On Demand	Manually
PBKDF (A3972)	KAT	CAST	On Demand	Manually
PBKDF (A3977)	KAT	CAST	On Demand	Manually
PBKDF (A3979)	KAT	CAST	On Demand	Manually
PBKDF (A3983)	KAT	CAST	On Demand	Manually
PBKDF (A3993)	KAT	CAST	On Demand	Manually
PBKDF (A4003)	KAT	CAST	On Demand	Manually
PBKDF (A4004)	KAT	CAST	On Demand	Manually
PBKDF (A4005)	KAT	CAST	On Demand	Manually
Counter DRBG (A3970)	KAT	CAST	On Demand	Manually
HMAC DRBG (A3970)	KAT	CAST	On Demand	Manually
KAS-FFC-SSC Sp800-56Ar3 (A3992)	KAT	CAST	On Demand	Manually
KAS-ECC-SSC Sp800-56Ar3 (A3962)	KAT	CAST	On Demand	Manually
KAS-ECC-SSC Sp800-56Ar3 (A3968)	KAT	CAST	On Demand	Manually
KAS-ECC-SSC Sp800-56Ar3 (A3977)	KAT	CAST	On Demand	Manually
KAS-ECC-SSC Sp800-56Ar3 (A3983)	KAT	CAST	On Demand	Manually
KAS-ECC-SSC Sp800-56Ar3 (A3993)	KAT	CAST	On Demand	Manually
KAS-ECC-SSC Sp800-56Ar3 (A4003)	KAT	CAST	On Demand	Manually
KAS-ECC-SSC Sp800-56Ar3 (A4004)	KAT	CAST	On Demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
KAS-ECC-SSC Sp800-56Ar3 (A4005)	KAT	CAST	On Demand	Manually
HMAC-SHA3-512 (A3964)	KAT	CAST	On Demand	Manually
HMAC-SHA3-512 (A3972)	KAT	CAST	On Demand	Manually
HMAC-SHA3-512 (A3979)	KAT	CAST	On Demand	Manually
RSA SigGen (FIPS186-4) (A3962)	KAT	CAST	On Demand	Manually
RSA SigGen (FIPS186-4) (A3977)	KAT	CAST	On Demand	Manually
RSA SigGen (FIPS186-4) (A3983)	KAT	CAST	On Demand	Manually
RSA SigGen (FIPS186-4) (A3993)	KAT	CAST	On Demand	Manually
RSA SigGen (FIPS186-4) (A4003)	KAT	CAST	On Demand	Manually
RSA SigGen (FIPS186-4) (A4004)	KAT	CAST	On Demand	Manually
RSA SigGen (FIPS186-4) (A4005)	KAT	CAST	On Demand	Manually
RSA SigVer (FIPS186-4) (A3962)	KAT	CAST	On Demand	Manually
RSA SigVer (FIPS186-4) (A3977)	KAT	CAST	On Demand	Manually
RSA SigVer (FIPS186-4) (A3983)	KAT	CAST	On Demand	Manually
RSA SigVer (FIPS186-4) (A3993)	KAT	CAST	On Demand	Manually
RSA SigVer (FIPS186-4) (A4003)	KAT	CAST	On Demand	Manually
RSA SigVer (FIPS186-4) (A4004)	KAT	CAST	On Demand	Manually
RSA SigVer (FIPS186-4) (A4005)	KAT	CAST	On Demand	Manually
ECDSA SigGen (FIPS186-4) (A3962)	KAT	CAST	On Demand	Manually
ECDSA SigGen (FIPS186-4) (A3964)	KAT	CAST	On Demand	Manually
ECDSA SigGen (FIPS186-4) (A3966)	KAT	CAST	On Demand	Manually
ECDSA SigGen (FIPS186-4) (A3967)	KAT	CAST	On Demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
ECDSA SigGen (FIPS186-4) (A3972)	KAT	CAST	On Demand	Manually
ECDSA SigGen (FIPS186-4) (A3977)	KAT	CAST	On Demand	Manually
ECDSA SigGen (FIPS186-4) (A3979)	KAT	CAST	On Demand	Manually
ECDSA SigGen (FIPS186-4) (A3983)	KAT	CAST	On Demand	Manually
ECDSA SigGen (FIPS186-4) (A3993)	KAT	CAST	On Demand	Manually
ECDSA SigGen (FIPS186-4) (A4003)	KAT	CAST	On Demand	Manually
ECDSA SigGen (FIPS186-4) (A4004)	KAT	CAST	On Demand	Manually
ECDSA SigGen (FIPS186-4) (A4005)	KAT	CAST	On Demand	Manually
ECDSA SigVer (FIPS186-4) (A3962)	KAT	CAST	On Demand	Manually
ECDSA SigVer (FIPS186-4) (A3964)	KAT	CAST	On Demand	Manually
ECDSA SigVer (FIPS186-4) (A3966)	KAT	CAST	On Demand	Manually
ECDSA SigVer (FIPS186-4) (A3967)	KAT	CAST	On Demand	Manually
ECDSA SigVer (FIPS186-4) (A3972)	KAT	CAST	On Demand	Manually
ECDSA SigVer (FIPS186-4) (A3977)	KAT	CAST	On Demand	Manually
ECDSA SigVer (FIPS186-4) (A3979)	KAT	CAST	On Demand	Manually
ECDSA SigVer (FIPS186-4) (A3983)	KAT	CAST	On Demand	Manually
ECDSA SigVer (FIPS186-4) (A3993)	KAT	CAST	On Demand	Manually
ECDSA SigVer (FIPS186-4) (A4003)	KAT	CAST	On Demand	Manually
ECDSA SigVer (FIPS186-4) (A4004)	KAT	CAST	On Demand	Manually
ECDSA SigVer (FIPS186-4) (A4005)	KAT	CAST	On Demand	Manually
Safe Primes Key Generation (A3992)	PCT	PCT	On Demand	Manually
RSA KeyGen (FIPS186-4) (A3962)	PCT	PCT	On Demand	Manually
RSA KeyGen (FIPS186-4) (A3977)	PCT	PCT	On Demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
RSA KeyGen (FIPS186-4) (A3983)	PCT	PCT	On Demand	Manually
RSA KeyGen (FIPS186-4) (A3993)	PCT	PCT	On Demand	Manually
RSA KeyGen (FIPS186-4) (A4003)	PCT	PCT	On Demand	Manually
RSA KeyGen (FIPS186-4) (A4004)	PCT	PCT	On Demand	Manually
RSA KeyGen (FIPS186-4) (A4005)	PCT	PCT	On Demand	Manually
ECDSA KeyGen (FIPS186-4) (A3962)	PCT	PCT	On Demand	Manually
ECDSA KeyGen (FIPS186-4) (A3966)	PCT	PCT	On Demand	Manually
ECDSA KeyGen (FIPS186-4) (A3977)	PCT	PCT	On Demand	Manually
ECDSA KeyGen (FIPS186-4) (A3983)	PCT	PCT	On Demand	Manually
ECDSA KeyGen (FIPS186-4) (A3993)	PCT	PCT	On Demand	Manually
ECDSA KeyGen (FIPS186-4) (A4003)	PCT	PCT	On Demand	Manually
ECDSA KeyGen (FIPS186-4) (A4004)	PCT	PCT	On Demand	Manually
ECDSA KeyGen (FIPS186-4) (A4005)	PCT	PCT	On Demand	Manually

Table 25: Conditional Periodic Information

The module does not implement periodic self-tests.

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
Error	The module immediately stops functioning	Software integrity test failure CAST failure PCT failure	Re-initialization of the module	Module will not load; Module is aborted for PCT failure

Table 26: Error States

If the module fails any of the self-tests, the module enters the error state. In the error state, the module immediately stops functioning and ends the application process. Consequently, the data output interface is inhibited, and the module accepts no more inputs or requests (as the module is no longer running).

Regarding the PCT failure, an `OSSL_PROV_PARAM_STATUS` parameter can be queried from the FIPS provider to check the status of the cryptographic module.

The table above lists the error states and the status indicator values that explain the error that has occurred.

10.5 Operator Initiation of Self-Tests

The software integrity tests and cryptographic algorithm self-tests can be invoked on demand by resetting the module or by invoking the `OSSL_PROVIDER_self_test` method. The pair-wise consistency tests can be invoked on demand by requesting the key pair generation service.

10.6 Additional Information

Not applicable.

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

The binaries of the FIPS validated module are contained in the following Ubuntu packages for delivery:

- openssl-fips-module-3_3.0.5-0ubuntu0.1+Fips2.1_amd64.deb for X86_64
- openssl-fips-module-3_3.0.5-0ubuntu0.1+Fips2.1_arm64.deb for ARM64
- openssl-fips-module-3_3.0.5-0ubuntu0.1+Fips2.1_s390x.deb for s390x

Once the operating environment is configured following the instructions provided, the Crypto Officer can install the Ubuntu packages containing the module listed below - Ubuntu packages using the Advanced Package Tool (APT) with the following command:

```
$ sudo apt-get install openssl-fips-module-3
```

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 fails.

After the openssl-fips-module-3 package is installed, the Crypto Officer must execute the openssl list -providers command. The Crypto Officer must ensure that the FIPS provider is listed in the output as follows:

fips

name: Ubuntu 22.04 OpenSSL Cryptographic Module

version: 3.0.5-0ubuntu0.1+Fips2.1

status: active

The cryptographic boundary consists only of the FIPS provider as listed. If any other OpenSSL or third-party provider is invoked, the user is not interacting with the module specified in this Security Policy.

After, the module needs to be set to run in the FIPS validated configuration. This can be enabled automatically via the Ubuntu Advantage tool after attaching your subscription.

(1) To install the tool type the following commands:

```
$ sudo apt update
```

```
$ sudo apt install ubuntu-advantage-tools
```

(2) To activate the Ubuntu Pro subscription run:

```
$ sudo pro attach <your_pro_token>
```

(3) To enable Approved mode run:

```
$ sudo pro enable fips
```

(4) To verify that Approved mode is enabled run:

```
$ sudo pro status
```

The pro client will install the necessary packages for the Approved mode, including the kernel and the bootloader. After this step you **MUST reboot** to put the system into Approved mode. The reboot will boot into FIPS supported kernel and create the `/proc/sys/crypto/fips_enabled` entry which tells the FIPS certified modules to run in Approved mode. If you do not reboot after installing and configuring the bootloader, Approved mode is not yet enabled.

To verify that FIPS is enabled after the reboot check the `/proc/sys/crypto/fips_enabled` file and ensure it is set to 1. If it is set to 0, the FIPS modules will not run in Approved mode. If the file is missing, the FIPS kernel is not installed, you can verify that FIPS has been properly enabled with the `pro status` command.

11.2 Administrator Guidance

The Crypto Officer shall follow this Security Policy to configure the operational environment and install the module to be operated as a FIPS 140-3 validated module. In addition, the Crypto Officer shall consider the following requirements and restrictions provided in Section 2.7 when using the module.

11.3 Non-Administrator Guidance

There is no non-administrator guidance.

11.4 Design and Rules

Not applicable.

11.5 Maintenance Requirements

Not applicable.

11.6 End of Life

As the module does not persistently store SSPs, secure sanitization of the module consists of unloading the module. This will zeroize all SSPs in volatile memory. Then, if desired, the Ubuntu packages can be uninstalled from the Ubuntu 22.04 system.

11.7 Additional Information

Not applicable.

12 Mitigation of Other Attacks

12.1 Attack List

Certain cryptographic subroutines and algorithms are vulnerable to timing analysis. The module mitigates this vulnerability by using constant-time implementations. This includes, but is not limited to:

- Big number operations: computing GCDs, modular inversion, multiplication, division, and modular exponentiation (using Montgomery multiplication).
- Elliptic curve point arithmetic: addition and multiplication (using the Montgomery ladder).
- Vector-based AES implementations.

12.2 Mitigation Effectiveness

RSA, ECDSA, ECDH, and DH employ blinding techniques to further impede timing and power analysis.

12.3 Guidance and Constraints

No configuration is needed to enable the aforementioned countermeasures.

12.4 Additional Information

Not applicable.

Appendix A. Glossary and Abbreviations

AES	Advanced Encryption Standard
AES-NI	Advanced Encryption Standard New Instructions
API	Application Programming Interface
CAST	Cryptographic Algorithm Self-Test
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher Block Chaining
CCM	Counter with Cipher Block Chaining-Message Authentication Code
CFB	Cipher Feedback
CKG	Cryptographic Key Generation
CMAC	Cipher-based Message Authentication Code
CMVP	Cryptographic Module Validation Program
CPACF	CP Assist for Cryptographic Functions
CSP	Critical Security Parameter
CTR	Counter
CTS	Ciphertext Stealing
DH	Diffie-Hellman
DRBG	Deterministic Random Bit Generator
ECB	Electronic Code Book
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
ENT (NP)	Non-physical Entropy Source
EVP	Envelope
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

© 2024 Canonical Ltd. / atsec information security.

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

IKE	Internet Key Exchange
KAS	Key Agreement Scheme
KAT	Known Answer Test
KBKDF	Key-based Key Derivation Function
KMAC	KECCAK Message Authentication Code
KW	Key Wrap
KWP	Key Wrap with Padding
MAC	Message Authentication Code
NIST	National Institute of Science and Technology
OAEP	Optimal Asymmetric Encryption Padding
OFB	Output Feedback
PAA	Processor Algorithm Acceleration
PCT	Pair-wise Consistency Test
PBKDF2	Password-based Key Derivation Function v2
PKCS	Public-Key Cryptography Standards
PSS	Probabilistic Signature Scheme
RSADP	RSA Decryption Primitive
RSAEP	RSA Encryption Primitive
RSA	Rivest, Shamir, Addleman
SHA	Secure Hash Algorithm
SSC	Shared Secret Computation
SSH	Secure Shell
SSP	Sensitive Security Parameter
TLS	Transport Layer Security
XOF	Extendable Output Function
XTS	XEX-based Tweaked-codebook mode with cipher text Stealing

Appendix B. References

- ANS X9.42-2001 **Public Key Cryptography for the Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography**
2001
<https://webstore.ansi.org/standards/ascx9/ansix9422001>
- ANS X9.63-2001 **Public Key Cryptography for the Financial Services Industry, Key Agreement and Key Transport Using Elliptic Curve Cryptography**
2001
<https://webstore.ansi.org/standards/ascx9/ansix9632001>
- 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)**
February 2023
<https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.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
<http://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 5288 **AES Galois Counter Mode (GCM) Cipher Suites for TLS**
August 2008
<https://www.ietf.org/rfc/rfc5288.txt>
- RFC 7919 **Negotiated Finite Field Diffie-Hellman Ephemeral Parameters for Transport Layer Security (TLS)**
August 2016
<https://www.ietf.org/rfc/rfc7919.txt>

RFC 8446	The Transport Layer Security (TLS) Protocol Version 1.3 August 2018 https://www.ietf.org/rfc/rfc8446.txt
SP 800-38A	Recommendation for Block Cipher Modes of Operation Methods and Techniques December 2001 https://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf
SP 800-38A 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 800-52r2	Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations August 2019 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r2.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 800-56Cr1	Recommendation for Key-Derivation Methods in Key-Establishment Schemes August 2020 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Cr1.pdf
SP 800-56Cr2	Recommendation for Key-Derivation Methods in Key-Establishment Schemes August 2020 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Cr2.pdf

SP 800-90Ar1	Recommendation for Random Number Generation Using Deterministic Random Bit Generators June 2015 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90Ar1.pdf
SP 800-90B	Recommendation for the Entropy Sources Used for Random Bit Generation January 2018 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90B.pdf
SP 800-108r1	NIST Special Publication 800-108 - Recommendation for Key Derivation Using Pseudorandom Functions August 2022 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-108r1.pdf
SP 800-132	Recommendation for Password-Based Key Derivation - Part 1: Storage Applications December 2010 https://csrc.nist.gov/publications/nistpubs/800-132/nist-sp800-132.pdf
SP 800-133r2	Recommendation for Cryptographic Key Generation June 2020 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-133r2.pdf
SP 800-135r1	Recommendation for Existing Application-Specific Key Derivation Functions December 2011 https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-135r1.pdf
SP 800-140B	CMVP Security Policy Requirements March 2020 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-140B.pdf